AI BOX® 2.1

User Manual

Device setting Guide

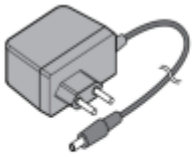
For AIBOX

Caution: The contents of this manual are subject to change at any time without prior notice.

Ⅰ. Overview

1. Components

Cable clamp

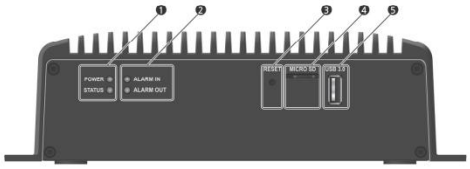


Adapter

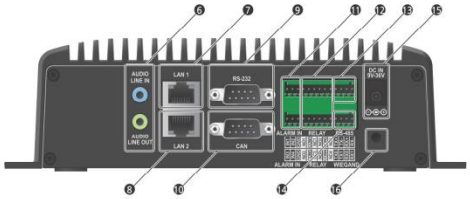
Screw

2. Names and Functions

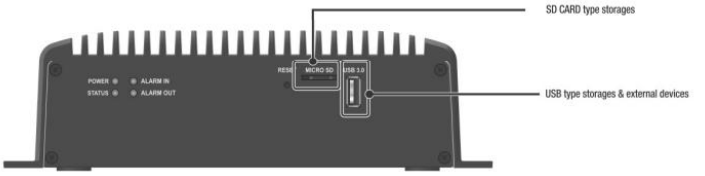
- Front View

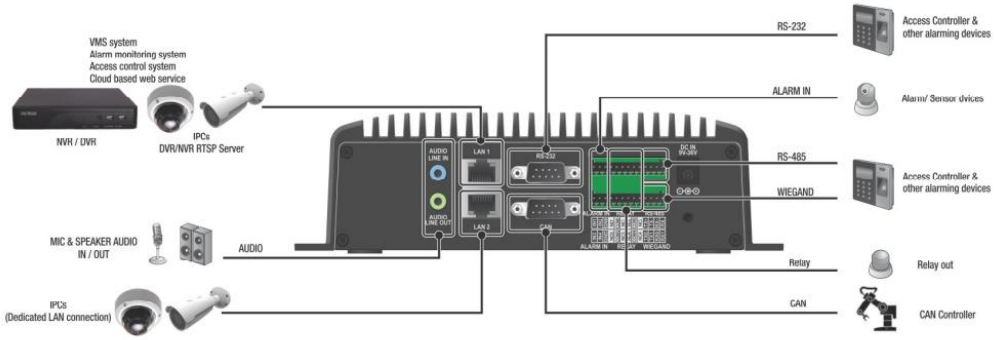


- Rear View



No.	Item	Description
❶	LED	Indicator LED for POWER / STATUS
❷	LED	Indicator LED for ALARM IN / ALARM OUT
❸	RESET	Factory reset button.
❹	MICRO SD	Slot for inserting a micro SD card.
❺	USB	Universal Serial Bus(USB) port for additional devices such as USB Memory Stick
❻	AUDIO	Connect the audio line input and output.
❼	LAN1	RJ-45 port for connecting internet and other platforms such as interoperable VMS, recorders and IP cameras.
❽	LAN2	RJ45 port for connecting IPCs and other devices through a separate LAN.
❾	RS-232	Connect the remote control device for RS232 communication.
❿	CAN	Connect the remote control device for CAN communication.
⓫	ALARM IN	Connect the sensor / alarm input signal wires.
⓬	RELAY OUT	Connect the relay output signal wire.
⓭	RS-485	Connect the remote control device for RS-485 communication.
⓮	WIEGAND	Connect the Wiegand input and output signal wires.
⓯	DC JACK	Connect the power plug of the provided 12V adapter.
⓰	CLAMP HOLE	DC JACK cable clamp fixed hole



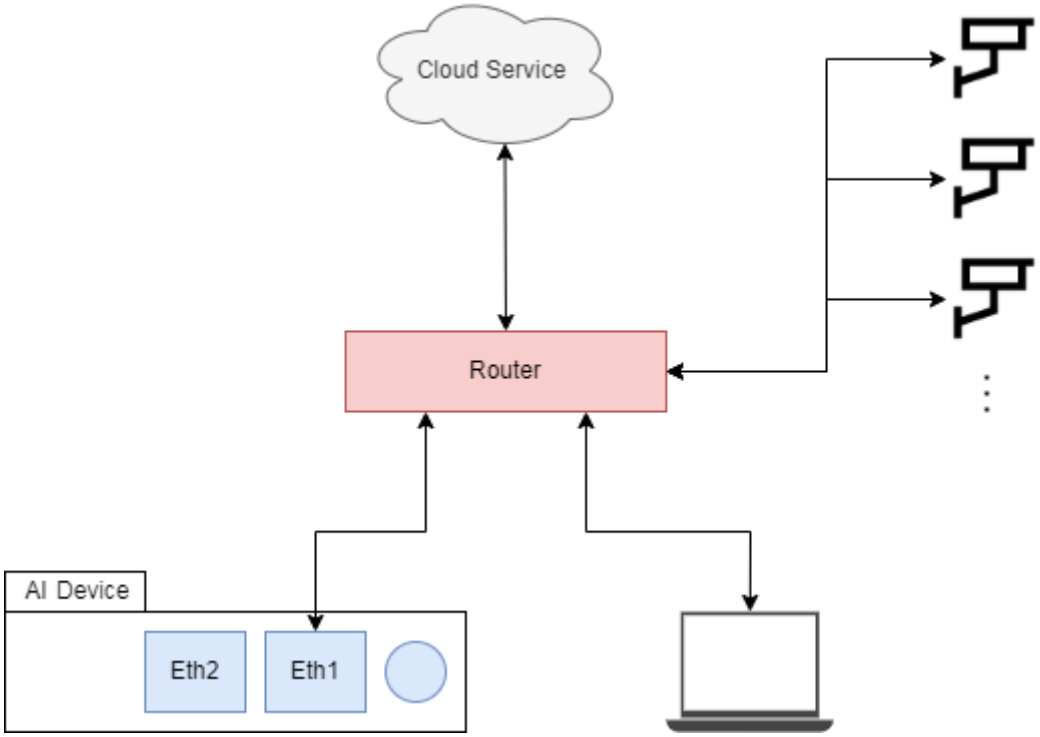


Ⅱ. AIBOX Settings

AIBOX is an AI video analysis device that analyzes multi-channel video using various types of AI algorithms to extract meaningful objects or identify various situations visually detected on the screen.
AI algorithms can be used to extract objects and follow the event after judging the situation with AI metadata. Based on AI analytics information, event condition and alarm types can be set as wanted. You can also accumulate and visualize your data to create analytical data that enables you to gain insights from continuous, otherwise meaningless data.
The document below explains the basic connection method of AIBOX, the structure of the system setting UI, and the setting method.

1. Device installation

1.1 Installing the AIBOX



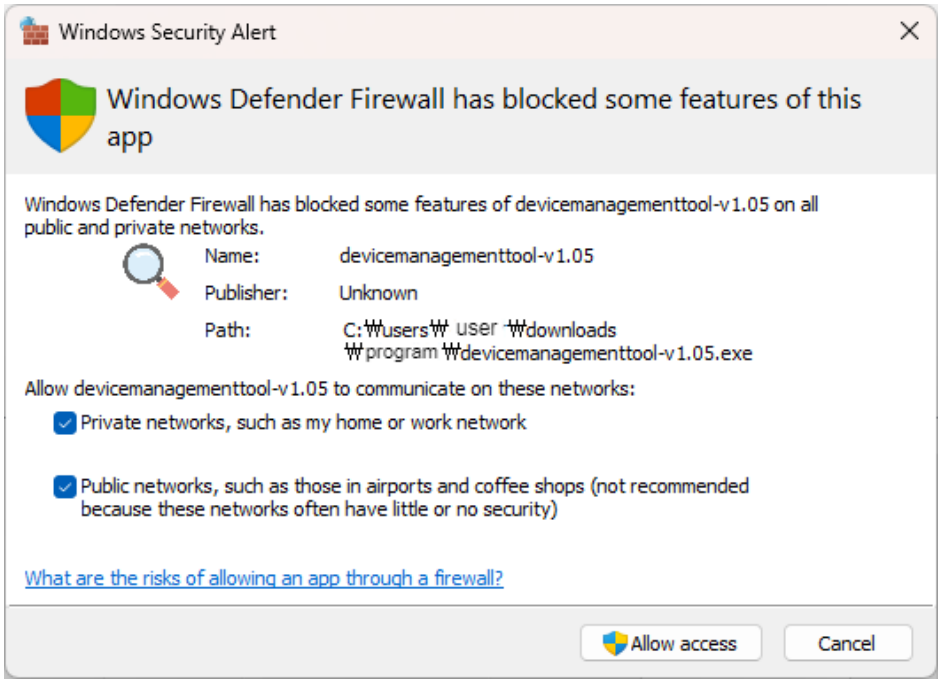
1. Install AIBOX on a network connected to the Internet and run a DHCP server.
2. Connect the network cable to ETHERNET 1 port of AIBOX.
3. The AIBOX boots up immediately when the adapter is powered on due to there not have separate power button.
4. It takes about 1 minute to connect to the PC after the device completes booting.

2. Search for devices on the network

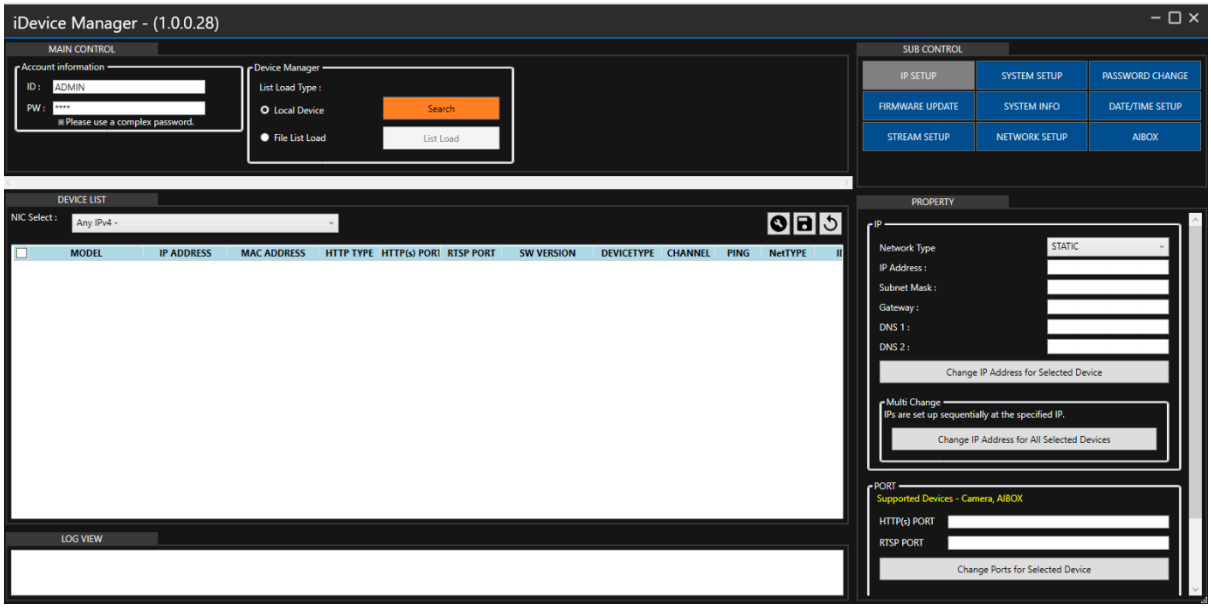
2.1 Download iDevice Manager

Download and install iDevice Manager from www.ganzsecurity.it . AIBOX is possible to search for the device's IP and set the network via iDevice Manager

When the install file runs, the firewall setting window will appear as below. For smoothly using, it is recommended to allow the entire network.

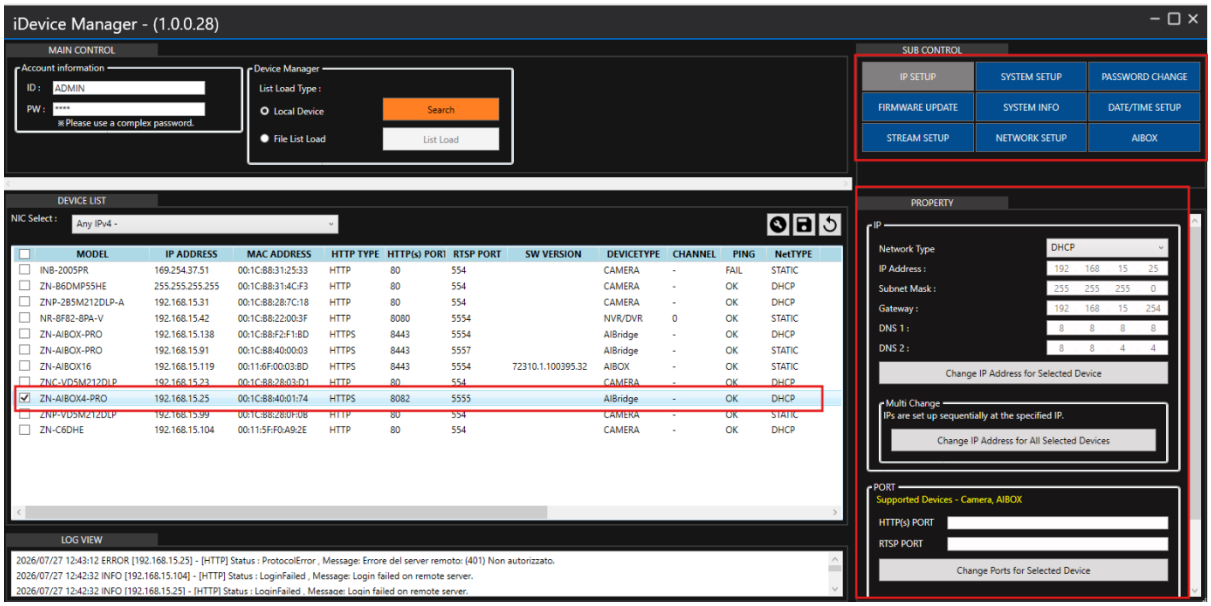


2.2 Running screen



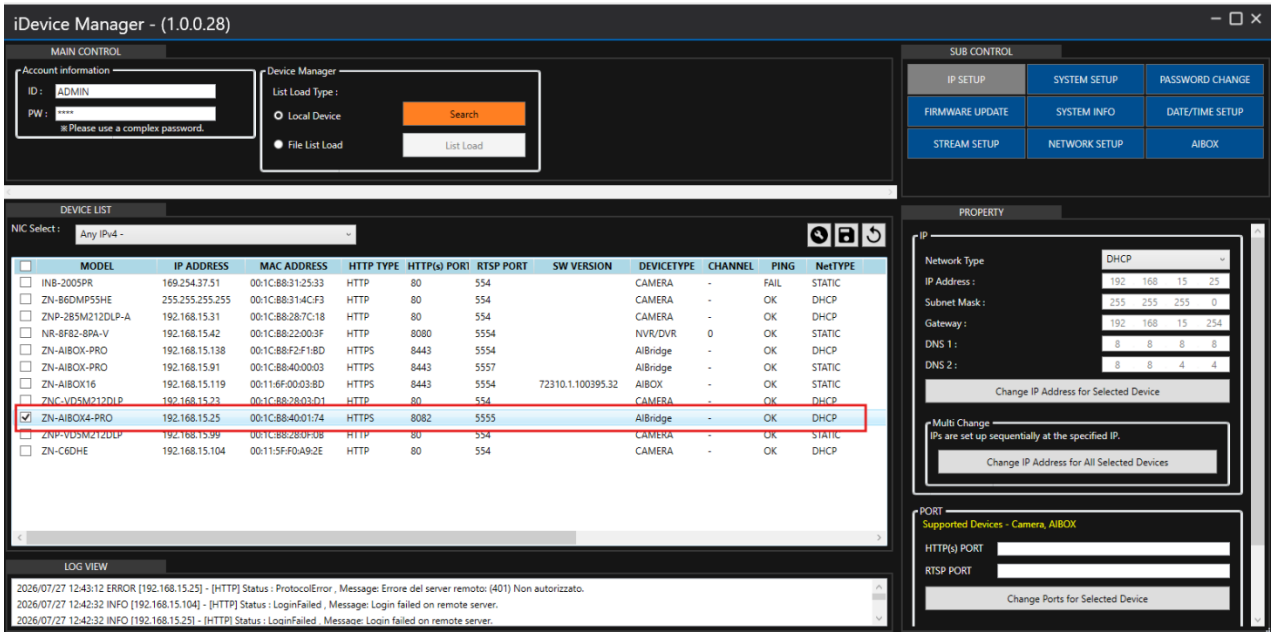
- When run for the first time, it shows a list of AIBOXs connected to the network. In the ID / Password field, admin / 1234 is entered by default.
- **When the AIBOX is in “factory default or factory reset” status, “1234” is set as a temporary password for network settings in the tool**
- If the AIBOX is not shown, please check the network cable is connected to ETHERNET 1 properly.

2.3 Setting screen



1. Click the device that wants to change the network settings from the list.
2. Enter the network information to set in the Setup Network section below.
3. Enter the ID / Password of the device.
   - If the AIBOX is in “factory default or factory reset”, enter admin / 1234.
4. Click the Apply button.

2.4 Screen after settings applied

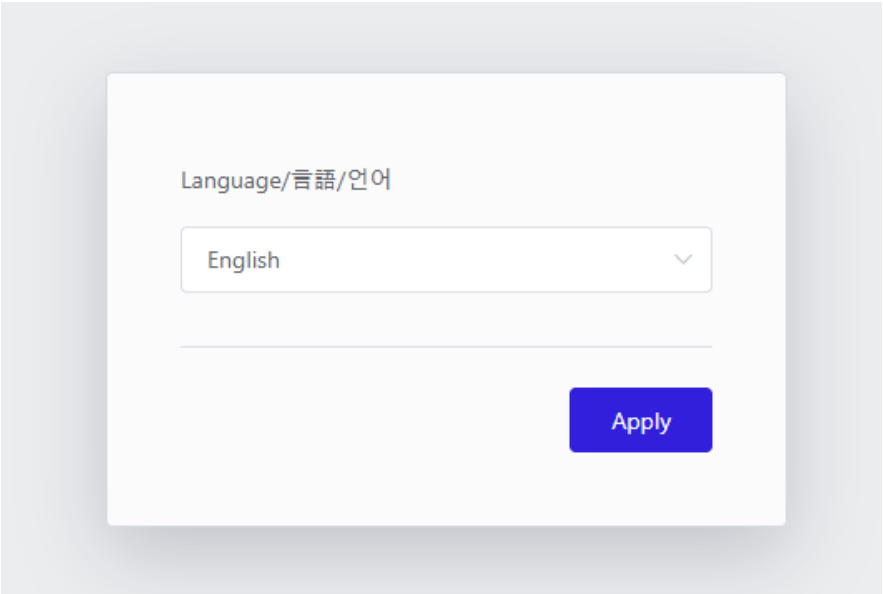


1. After a while by pressing the Apply button, the network setting of the device will be updated in the list.
- If the network settings have not been changed, it is due ID or Password being incorrect, please check again.
2. After setting up the network, double-click the device information in the list to access the AIBOX.
- The AIBOX webpage will open in the default browser in Windows.

3. Initial access settings

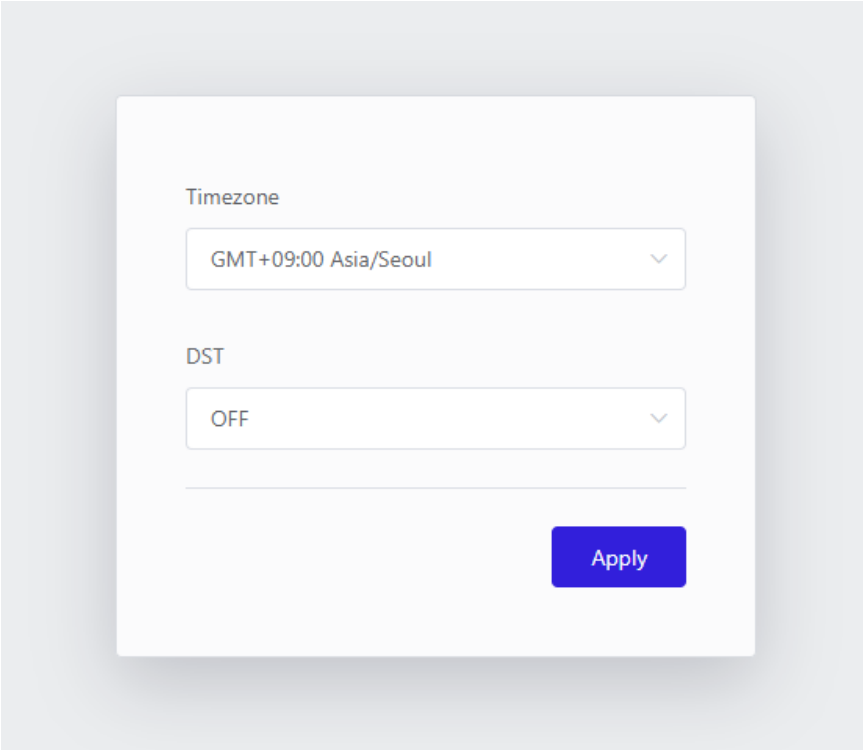
When accessing the AIBOX for the first time, the initial setting wizard is displayed.
To use the AIBOX, complete the setup in the order shown in the UI.

3.1 Device language settings



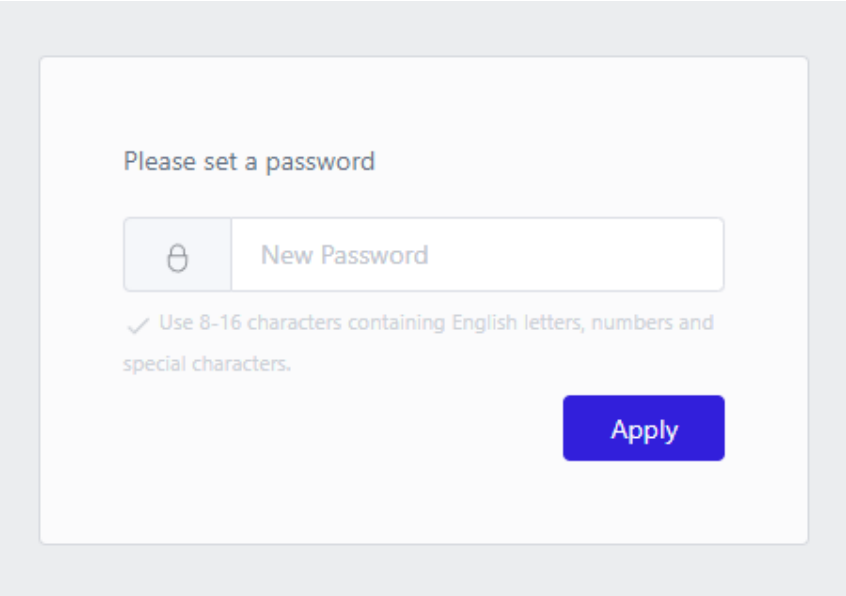
The appropriate language is set as the default to match your browser's language settings. If you want a different language, select the desired language from the drop-down box.

3.2 Device Time-zone settings



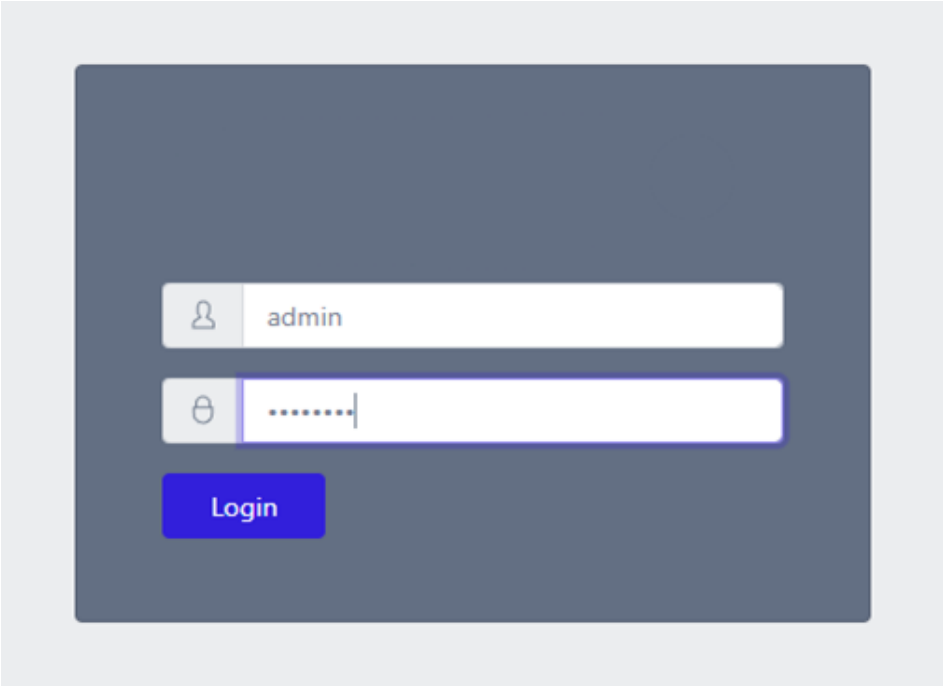
Set the password I want to use. The password can use the alphabet, numbers, and special characters, and it should be set to 8 to 16 characters.

3.3 Initial password setting of Device



When accessing the AIBOX for the first time, the initial password setting UI is displayed. Set the password I want to use.
The password can use the alphabet, numbers, and special characters, and it should be set to 8 to 16 characters.

3.4 Accessing to Device and setting the remote support settings

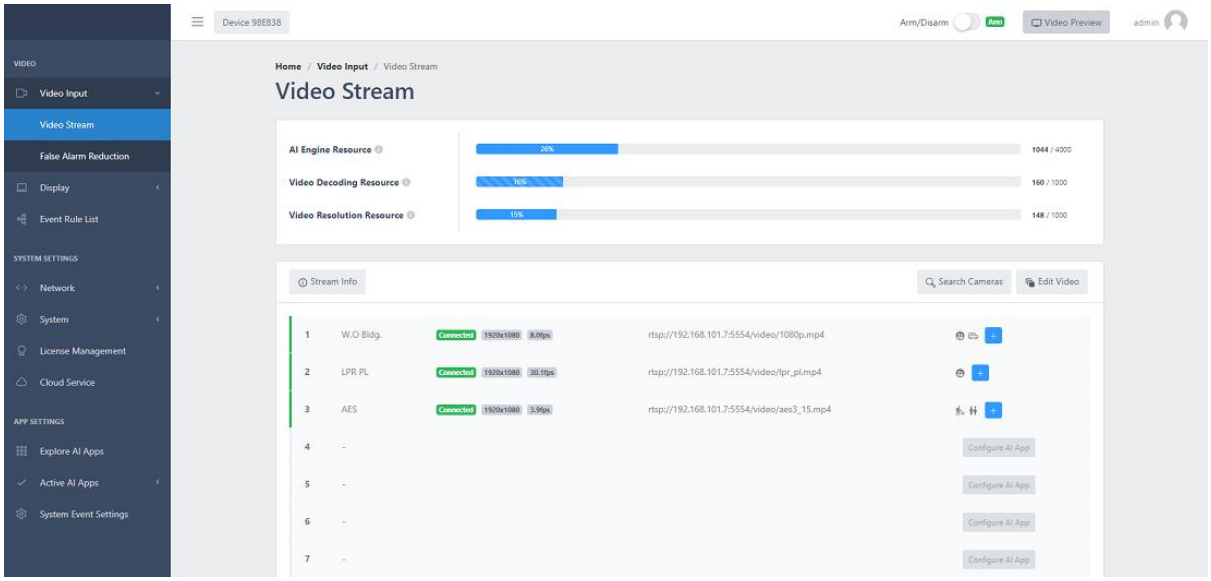


Log in using the device's account information using admin as the ID and the password set in the previous step.

4. Video source setup

4.1 Camera Video Input Setting

To enable the AIBOX to receive and analyze video from a camera, you must first set up the camera's connecting information.



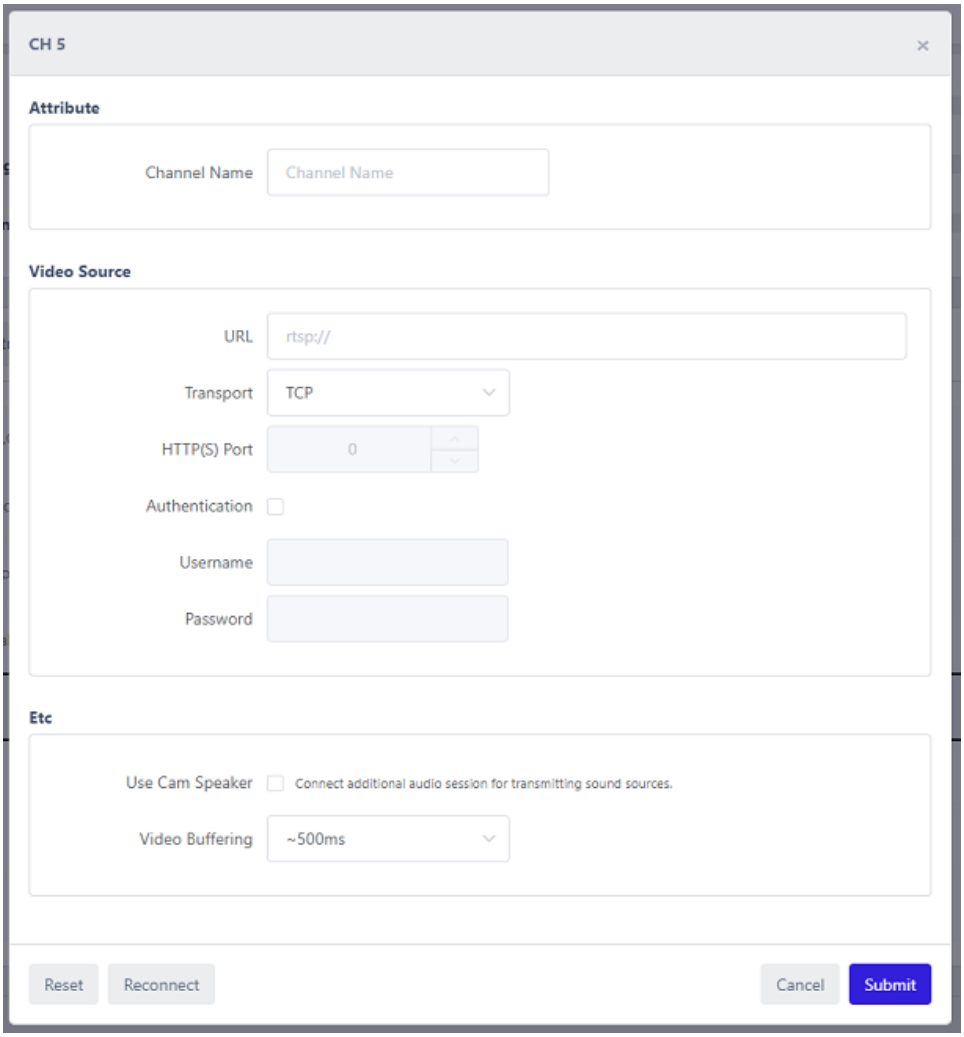
Click the **'Video Stream'** in the sidebar navigation menu displays the settings menu for receiving video from the camera.

① The **'AI Engine Resource'** displays usage relative to maximum AI processing capability. Each app requires a different AI processing capacity, so be careful not to set over the maximum processing.
The **'Video Decoding Resource'** shows current usage based on the maximum amount of video the AIBOX can receive and process from the camera. The **'Video Resolution Resource'** shows the usage against the maximum resolution available on the AIBOX. No item will exceed the limit.

② The **'Video Stream'** settings allow you to set the video stream information accessible over the network.

4.2 Video Stream for Each Channel Setting

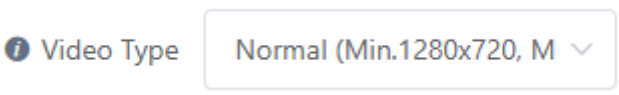
Click the **channel** for which you want to set the video in the list of video streams.



① Enter the **Channel Name**
② Enter the **RTSP URL** of the camera.
③ Select a transport protocol. The transport protocol specifies the protocol of the transport layer used to import the video stream.
④ Set the credentials needed for receiving the video stream. Usually, the ID and password of the IP camera are used.
⑤ If you want to use a camera speaker, check the **'Use Camera Speaker'.**
⑥ Set the maximum video buffering time. If, due to network conditions or camera types, video information is not transmitted smoothly and is received in a sudden burst, AIBOX can redistribute it into smooth videos according to the buffering setting. As the 'Video Buffering' setting is a maximum value, the actual buffering will be less than the set value if there are no problems with the camera and network performance.

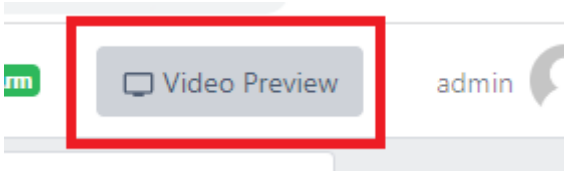
4.3 Change the Video Type

You can change the video type in the video stream for each channel setting. To check the video type, you can look near the other channel informations. Currently the types supported are Fisheye and Corridor Mode (max 720x1280).



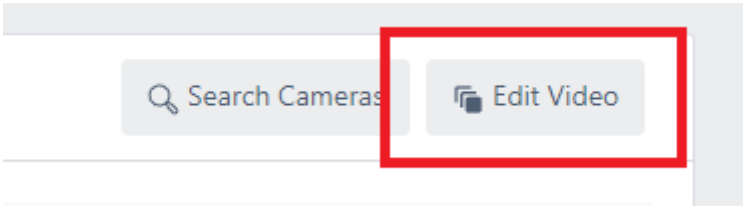
4.4 Check the Video Stream Connection Setting

You can check that the video stream you have set up is being received correctly. To check the receiving video stream, click the **'Video Preview'**.



4.5 Multiple video channels at once

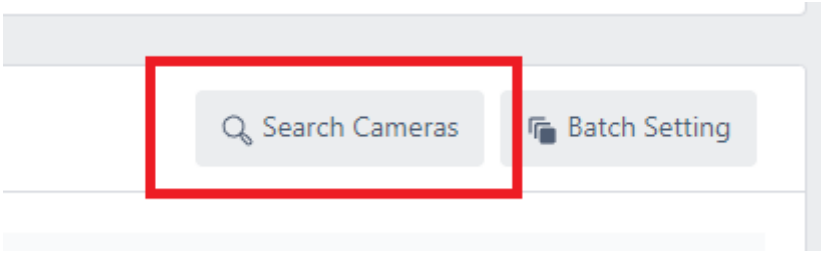
Set up multiple channels of video streams at once. You can set up multiple channels of video streams in bulk using copy and paste, as well as features such as Apply to All.
To use the Bulk Setup feature, click the **'Edit Video'** button in the Video Stream Settings area.



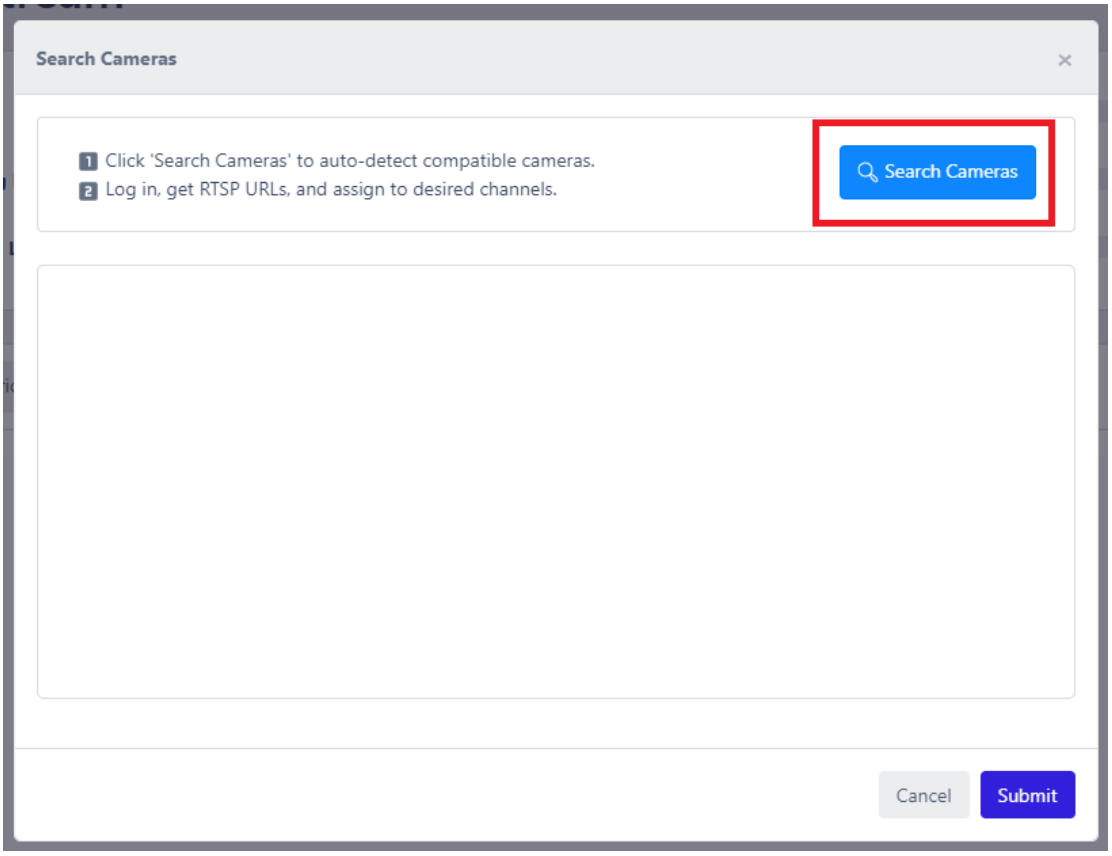
The 'Batch Setting' allows you to set the name, RTSP URL, transport, and authentication information for all channels at once.
The settings you enter in the Apply All line at the top can be applied to all channels by clicking the tick button for each setting.

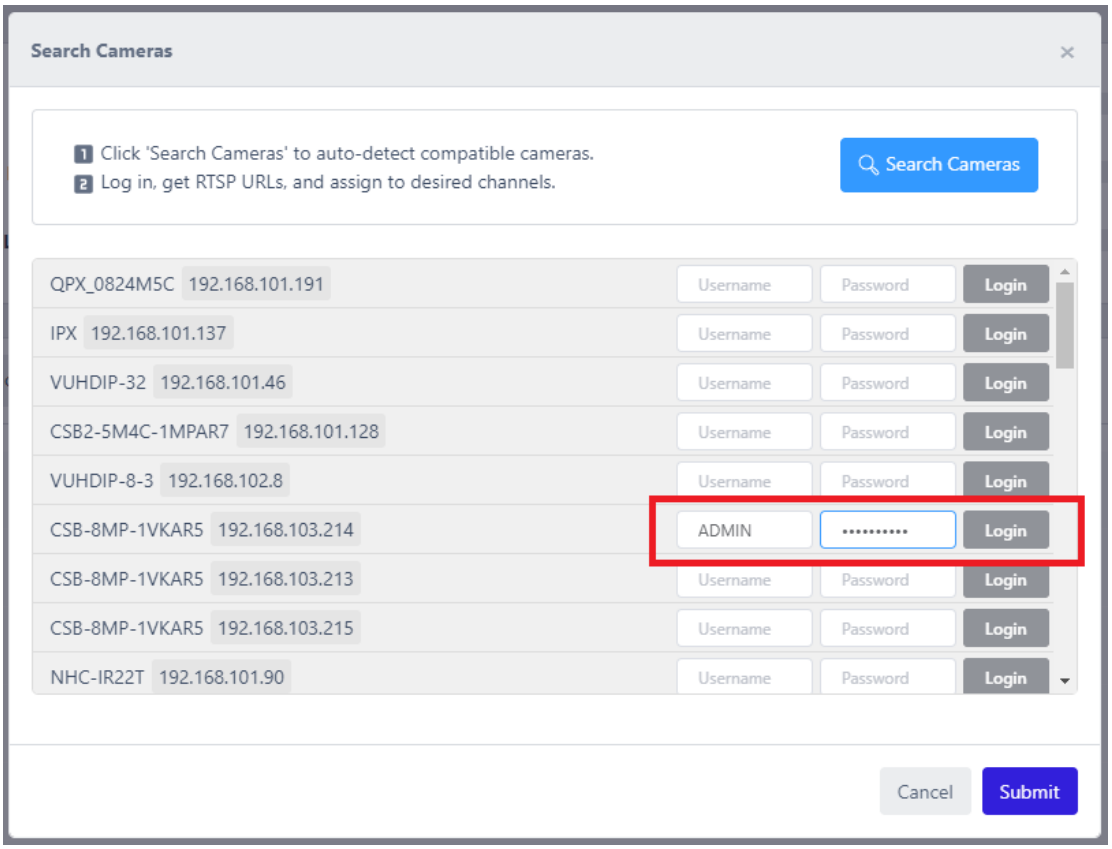
4.6 Searching for setting ONVIF cameras

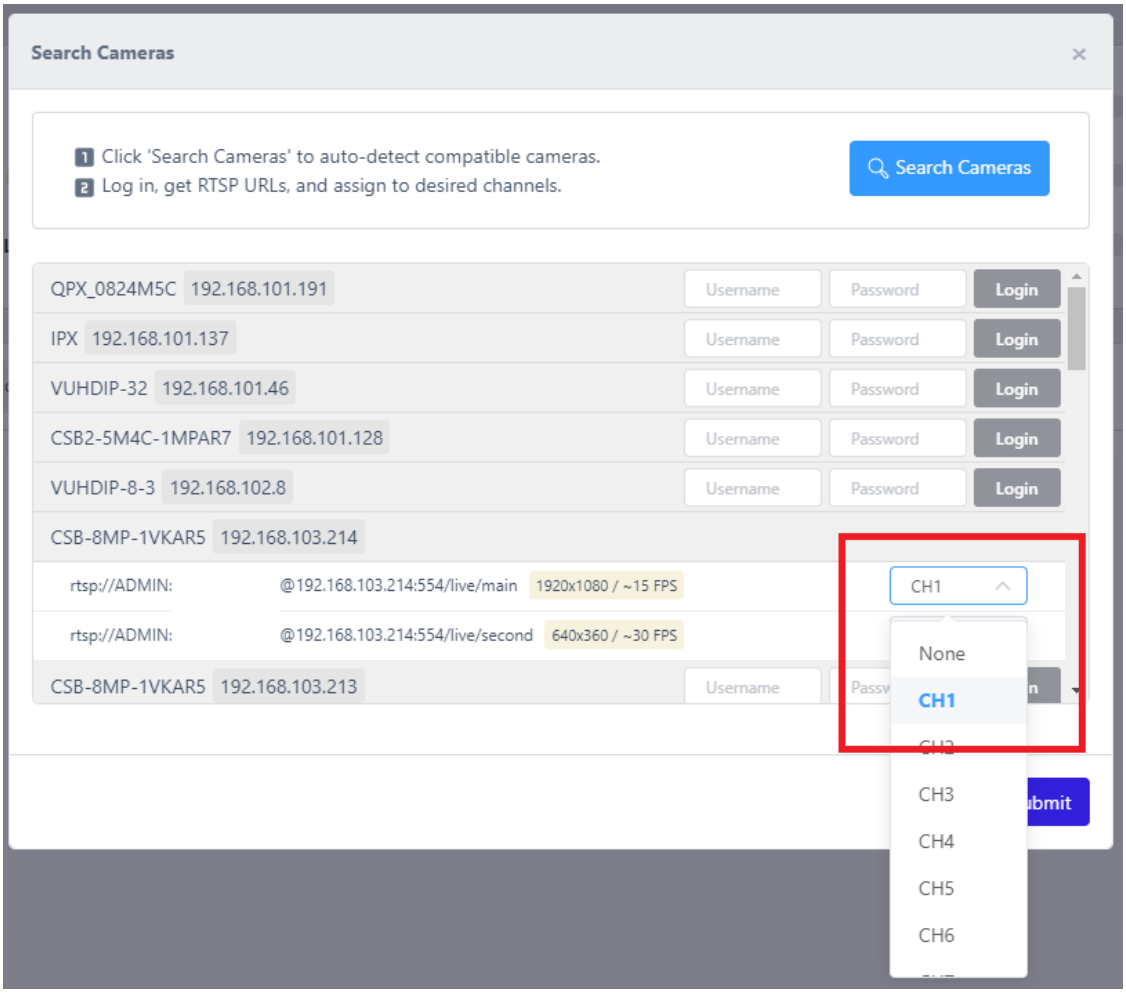
ONVIF is a standard for the interoperability of physical security devices. For network cameras that support the ONVIF standard, you can set up video streams using Discovery. To use the discovery feature, click the **'Search Cameras'**.



Search for your camera in the ONVIF search pop-up, then enter your credentials to see a list of video streams supported by your camera. Assign the streams you wish to analyze to a channel on the AIBOX.

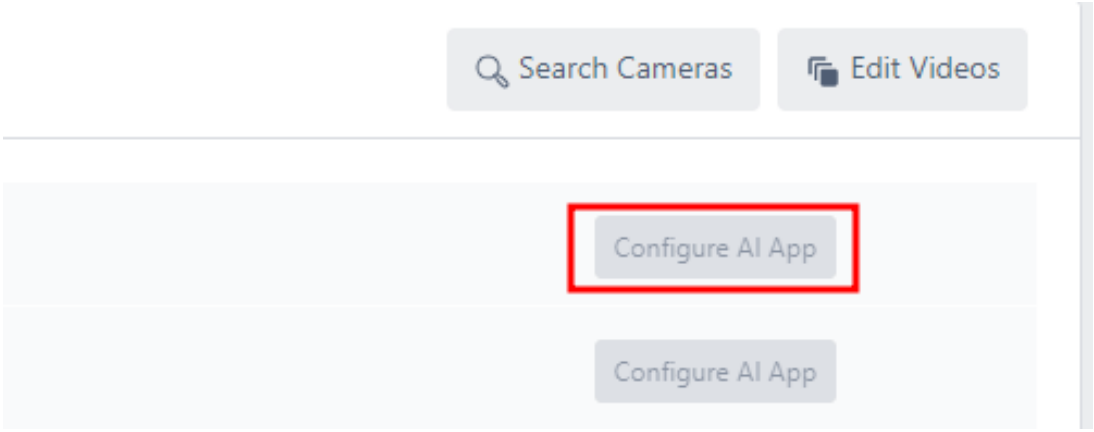

Search Cameras
1 Click 'Search Cameras' to auto-detect compatible cameras.
2 Log in, get RTSP URLs, and assign to desired channels.
Search Cameras
Cancel
Submit


Search Cameras
1 Click 'Search Cameras' to auto-detect compatible cameras.
2 Log in, get RTSP URLs, and assign to desired channels.
Search Cameras
QPX_0824M5C 192.168.101.191
IPX 192.168.101.137
VUHDIP-32 192.168.101.46
CSB2-5M4C-1MPAR7 192.168.101.128
VUHDIP-8-3 192.168.102.8
CSB-8MP-1VKAR5 192.168.103.214
CSB-8MP-1VKAR5 192.168.103.213
CSB-8MP-1VKAR5 192.168.103.215
NHC-IR22T 192.168.101.90
Username
Password
Login
ADMIN
Cancel
Submit



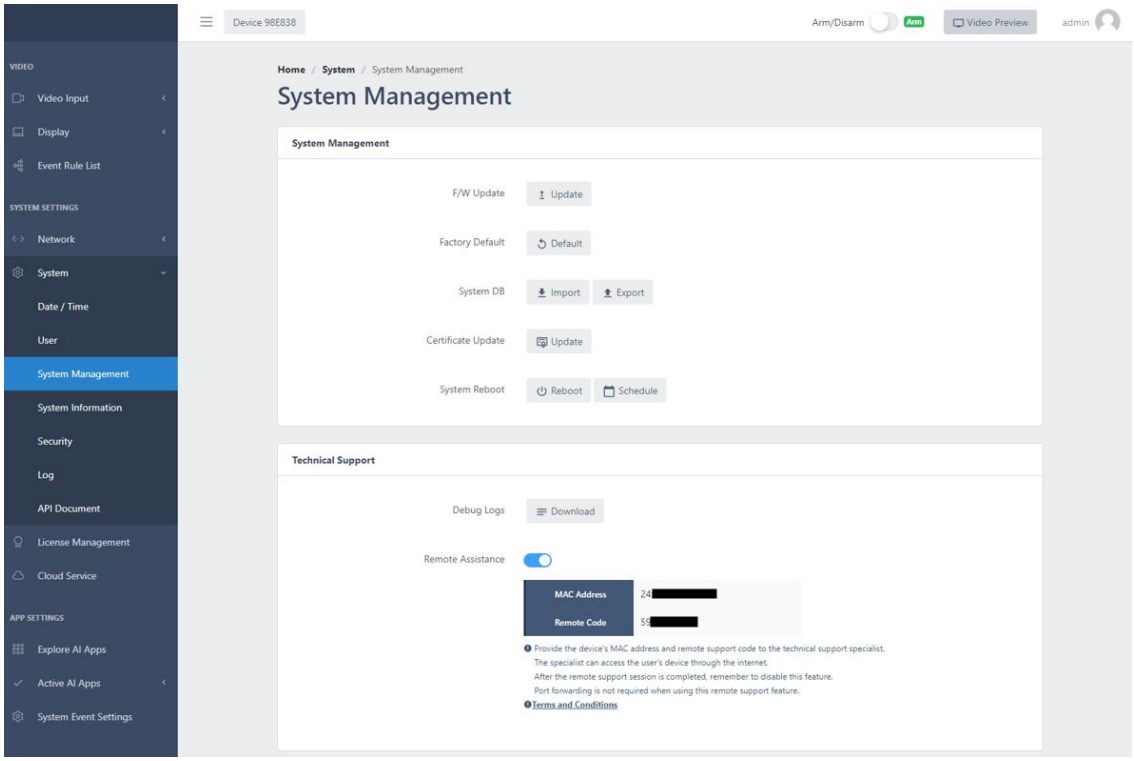
4.7 Searching for setting ONVIF cameras

Once the video stream is set up and connected, click the 'Configure AI App' button, select the appropriate app, and set the event action rule.



5. Remote support settings

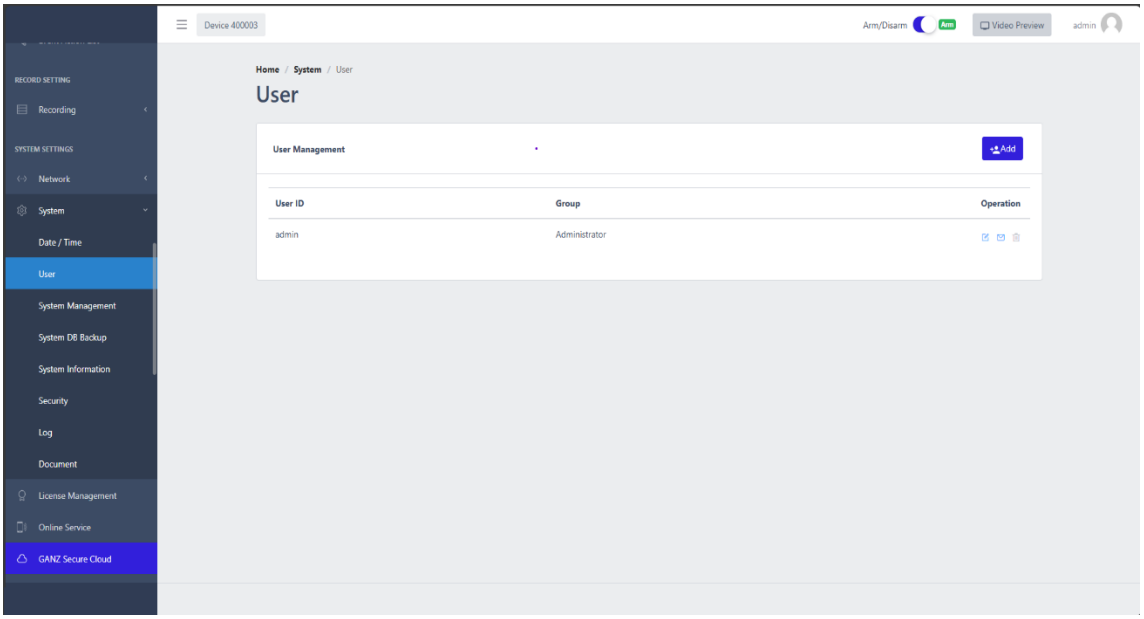
5.1 Remote support Settings



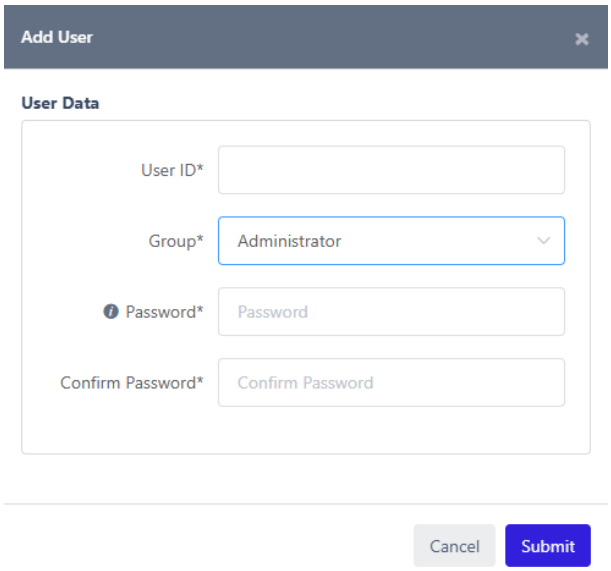
Enable the Remote Assistance function in the System > System Management > Technical Support menu. You can receive remote technical support by sharing the Mac Address and Remote Code displayed on the UI.

6. User creation settings

6.1 User creation settings



You can create multiple user with different authorizations. To do that, use the button Add to open a pop-up window with the user information.



The group determines what permissions a user can have and is composed of:

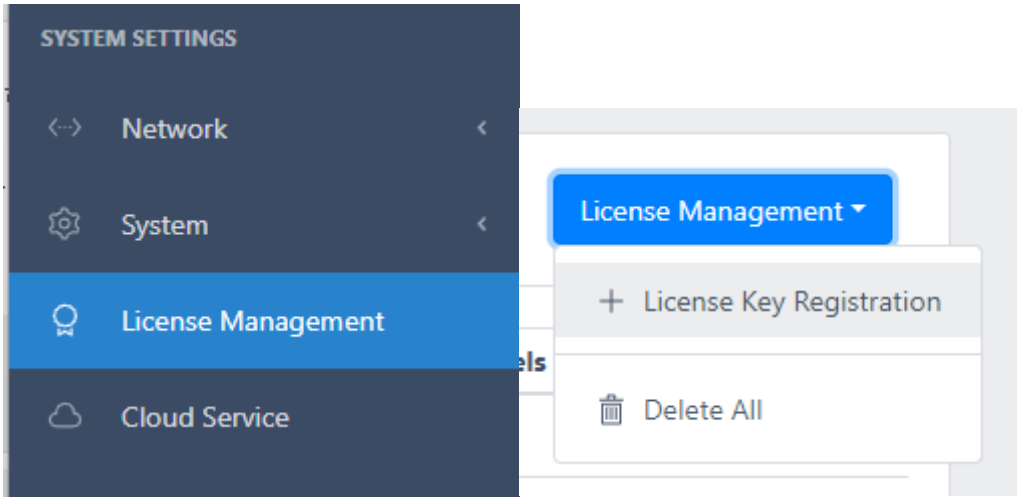
- **Administrator**: Has full authority. Can add or delete all registered users, including Administrator, Managers and Viewers.
  An Admin-level user created by the original Administrator can be deleted by that original Administrator.
  However, an additionally created Admin user cannot delete the original Administrator account.
- **Manager**: Has all permissions except for GDPR settings. Can add or delete other Manager-level users and can be deleted by an Administrator.
- **Viewer**: Can view all menus but does not have permission to add or delete users

Ⅱ. Application usage guide

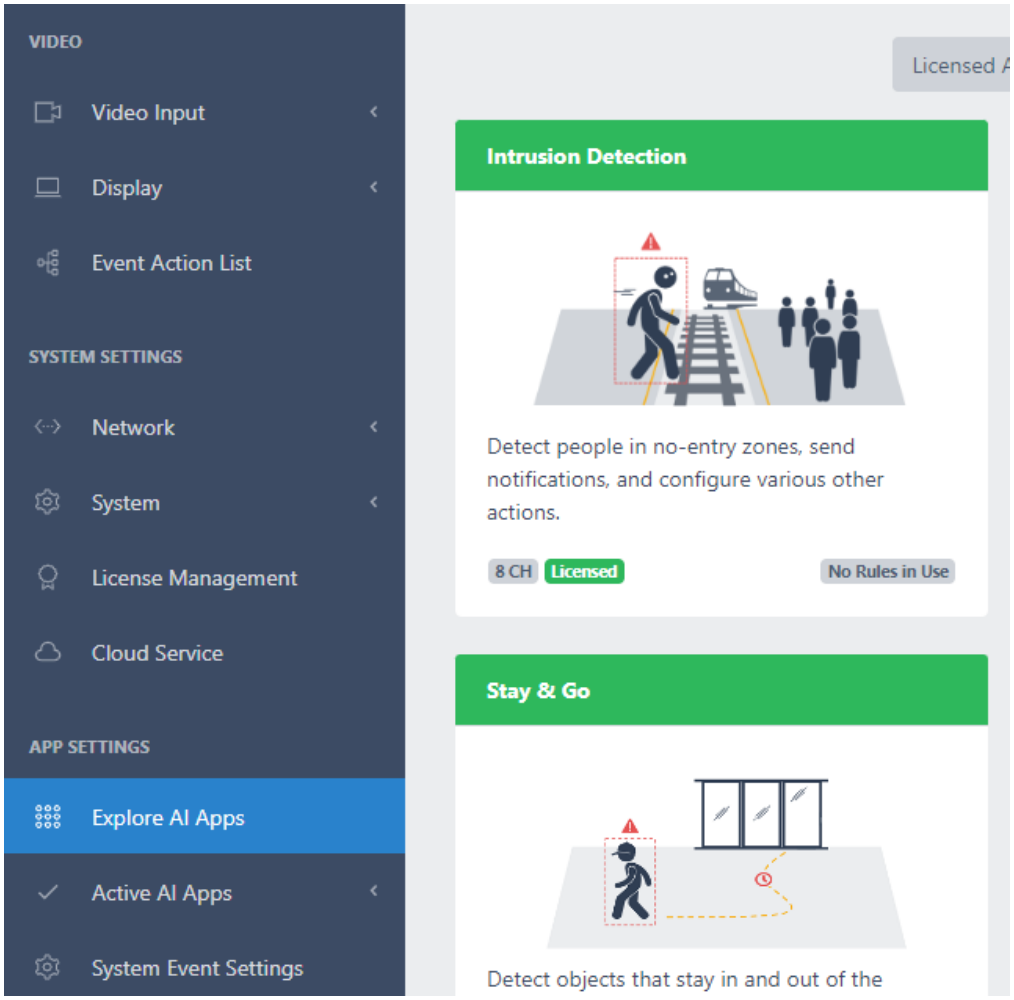
AIBOX works by adding various applications in the form of add-ons.
To add and use the application to the device, a license to use the application should be issued from the device dealer.

1. Application Activate

To activate additional apps, you need a license for each application.
Licenses are issued by the seller of the device in the form of a .json file, which you register and use in the 'License Management'.



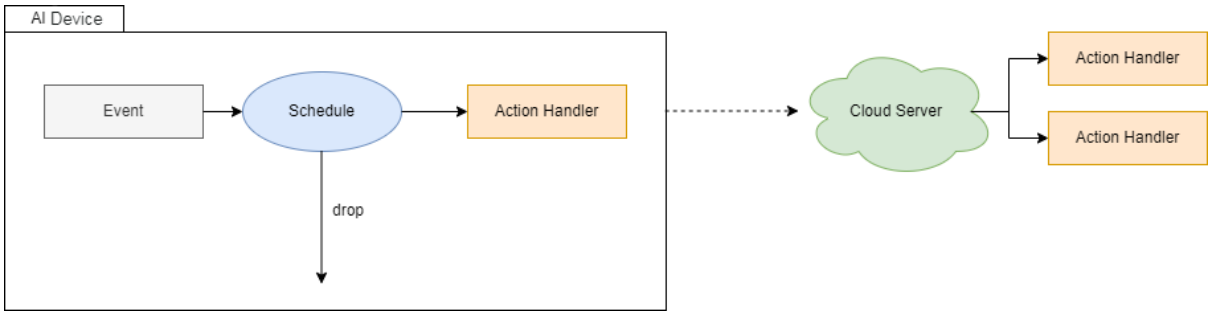
If the device has a license, the app will appear as a green header in the 'Explore AI apps' menu.



In the 'Explore AI apps', you can click on the app that you want to use to go to the settings menu for that app.

2. Event Action Setting Guide

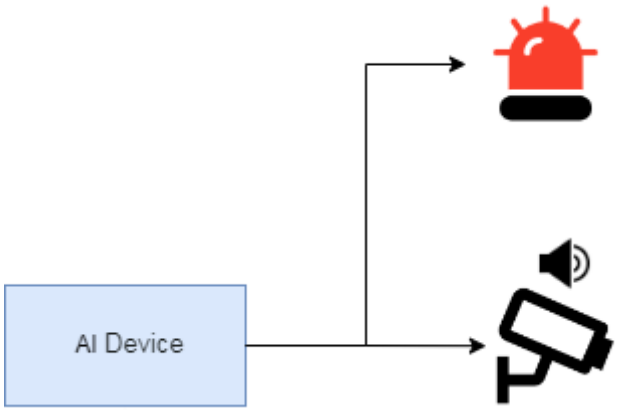
Many of the various applications supported by AIBOX have a structure that performs predefined actions for events detected based on AI.
By defining events and setting related actions, notification on real-time events can be used for a variety of purposes.



When an event is triggered by the event action setting, the schedule is checked. If the event occurs at other times with the schedule, the event is dropped without any event action.

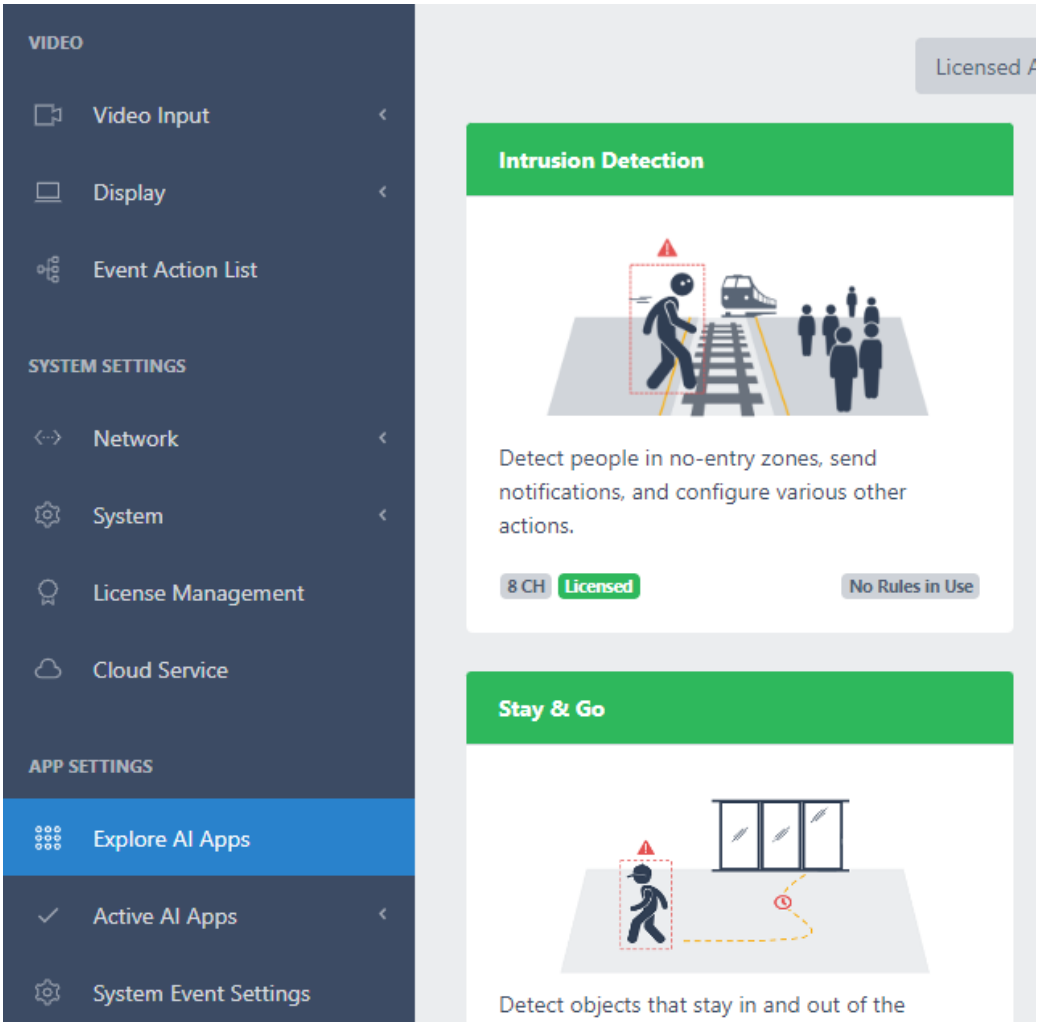
If the action run time is set, the action that can be run on the edge is run first.

Using a cloud application is not mandatory, but it allows for performing more actions using the network.



2.1 Alarm setting example (Intrusion)

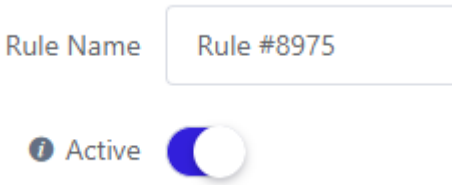
To set up an intrusion detection event action, click the **'Explore AI Apps – Intrusion Detection'** in the sidebar navigation menu.



To set a new detection rule, click the 

button in the intrusion detection settings.

2.1.1 Event Action Rules Setting

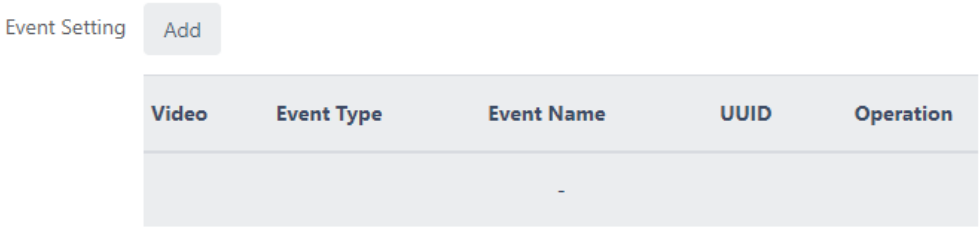


1. Enter a name for the rule. A random default value is entered, change this if necessary. You can also identify the rule by the name you enter in the action performed by the action handler.

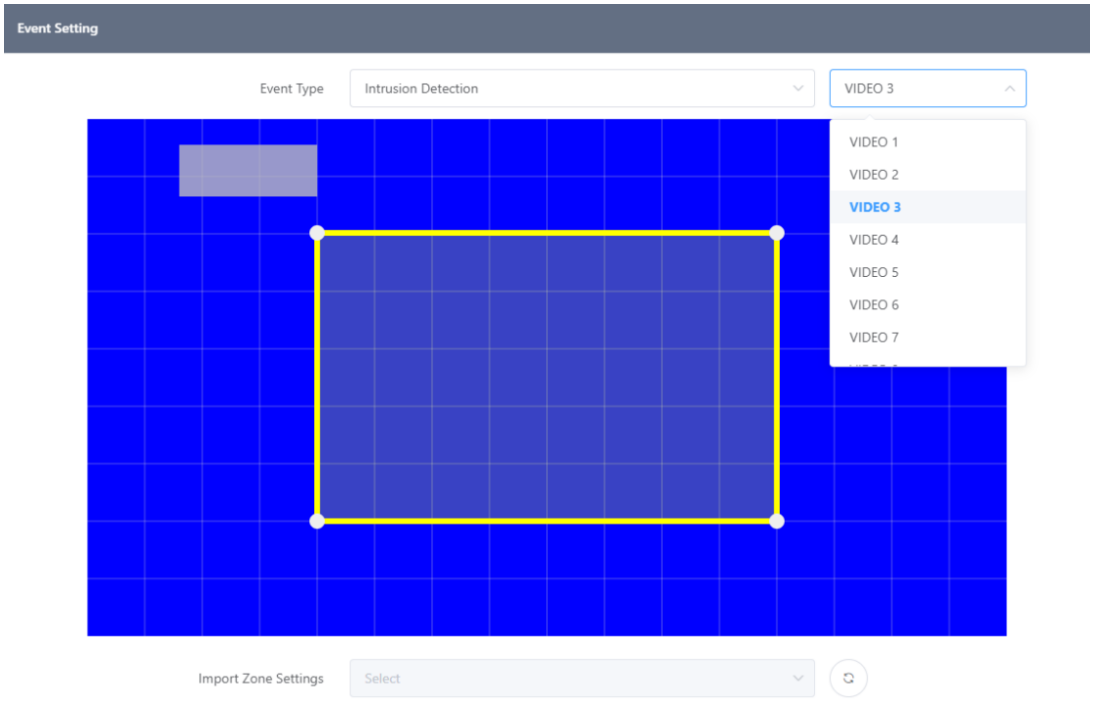
2. If you want to activate the event action rule upon creation, turn on the '**Active**' switch.

2.1.2 Event Setting

1. Click the Add button to set up the event.



2. Select the video want to detect via the dropdown to the right of the Event Type.

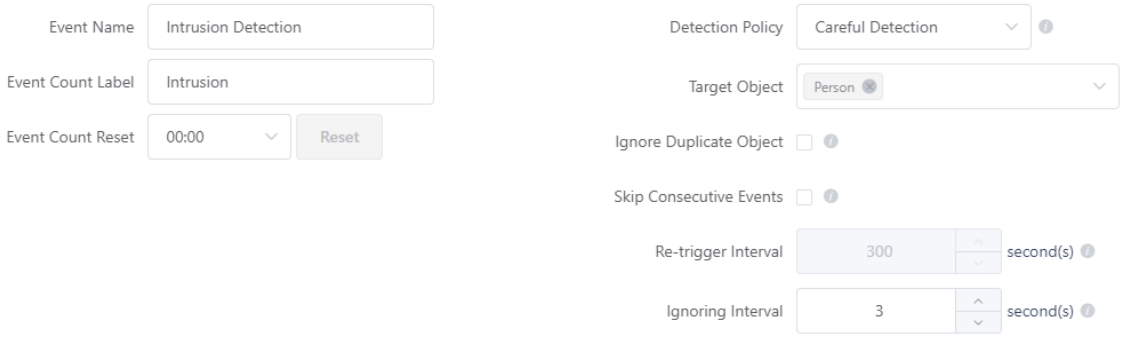


The detection zone can be set using the functions below. Alternatively, you can select zone information generated from other event settings by importing zone information.

- Drag the detection zone to **move the entire area**.
- Drag the **vertex to move** it.
- Click the yellow line to **add a new vertex** at that point.
- Right-click the vertex to remove it.
- Drag the gray box to move the label position.

After done, the video will look like below with the event zone ad label set up above.

3. Click the Apply & View button to save after setting for each option.



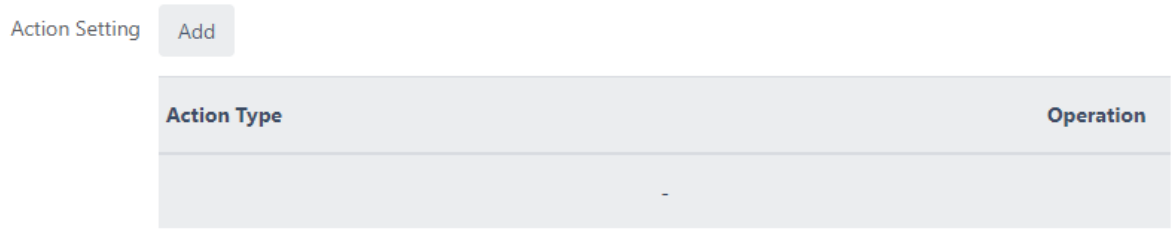
- Event Name : Enter the name of the event zone you created above.
- Detection Policy : Select whether to make event judgments about objects quickly or cautiously. When setting up a careful detection policy, objects are observed for a period of time to ensure that events are raised as accurately as possible. This can reduce false alarms at the expense of slightly delayed events. When setting a fast detection policy, the event is raised as soon as the object is detected. In this case, the time to observe the object is minimized in order to make a quick decision, which may result in false positives.
- Event Count Label : Enter the name of the label widget drawn over the video.
- Target Object : Select the event detection target. Person, Vehicle, and bike can be set.
- Event Count Reset : Set whether the event counts value or not. When enabled, the count value is reset at the set time.

- Ignore Duplicate Object : When checked, the same object will be ignored if it enters the event area again.
- Skip Consecutive Events : When checked, ignores events caused by new objects as long as the detected event target remains in the event zone.
- Re-trigger Interval : When Ignore Duplicate option is enabled, if there are still detected event targets in the zone, the event will occur again every set time.
- Ignoring Interval : Do not occur new events during the set time after an event occurs.

2.1.3 Action Settings

Define the event action to take when the event set occurs in Action Setting.

1. Click the Add button to add a new action item.

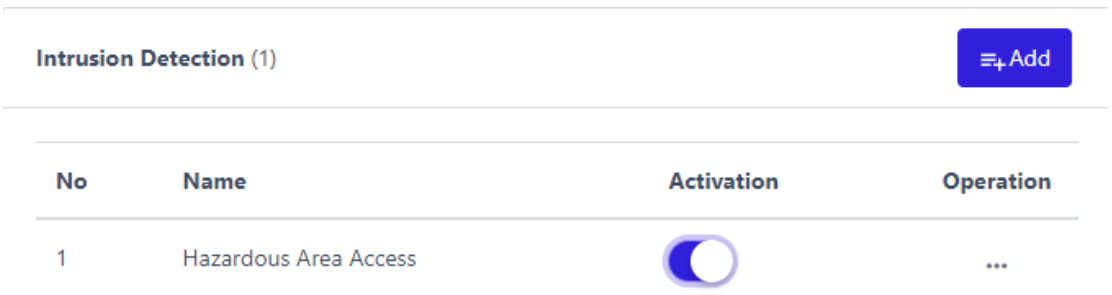


2. Set each action want to perform when an event occurs. Please refer to the Action setting Guide for the types of actions supported and how to set them up.

2.1.4 Finish setup

1. Click the Submit button at the very bottom to save intrusion detection event settings after setting up the event, action in the event action rule set page.

2. If everything is set up correctly, you can see the new event in the list on the Intrusion Detection application screen.



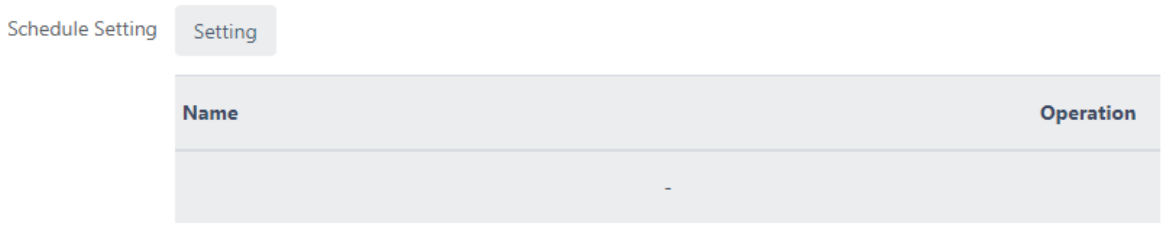
2.1.5 Filter settings (optional)

Schedule and Combined Rule filters can be used to set up event filters to drive actions. The schedule and Combined Rule filter settings described below are not required to configure an action rule, so you only need to set them if necessary.

2.1.5.1 Schedule settings

Set up event action schedules that operate over a period of time to set the time for sending the notification whenever an event occurs.

1. Click the Setting button to set the event action schedule.



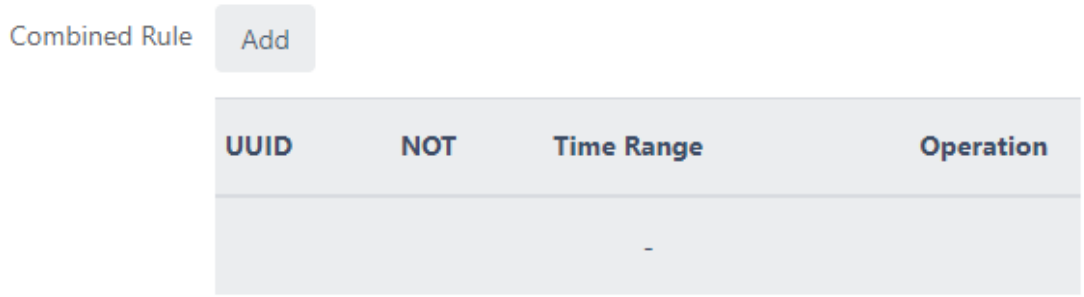
2. Add a schedule to drive action when an event occurs. Please refer to the '**Schedule Setting Guide**' for more information on how to set up a schedule.

2.1.5.2 Combined Rule condition settings

Set compound conditions on event actions to perform more complex forms of event filtering. The following items can be set as compound conditions.

- Rules set in the application in the form of an event action
- Events that make up a rule are set in an application in the form of an event action
- System I/O devices, such as alarm inputs or virtual alarm inputs

1. Click the Add button to set the combined rule condition.

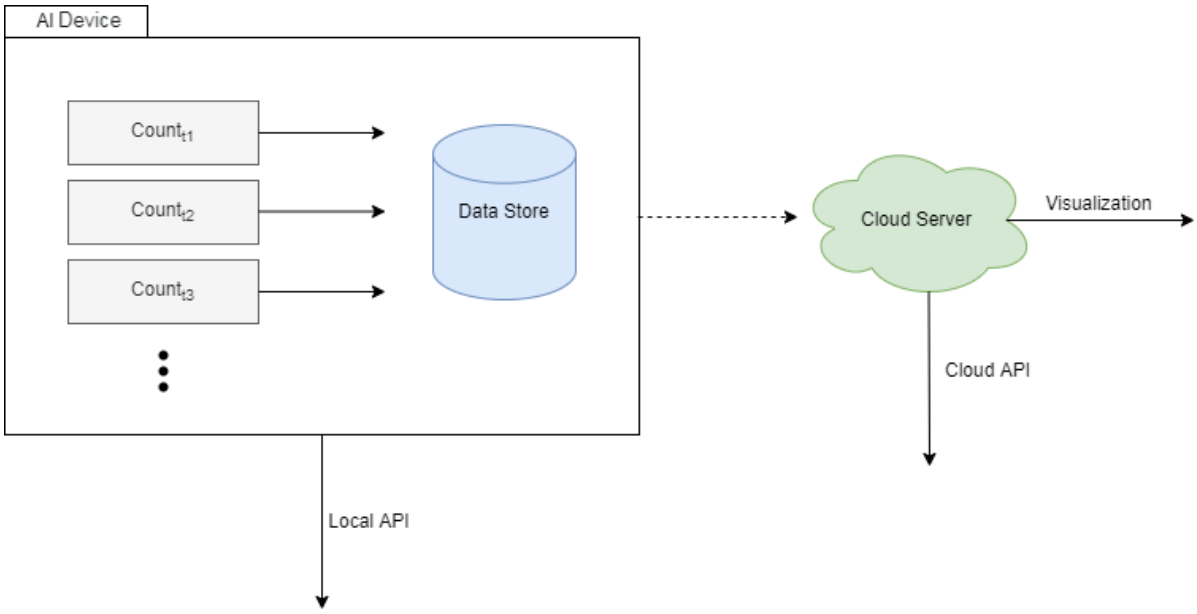


2. Please refer to the '**Combined Rule Setting Guide**' for more information on setting up.

3. Counter Setting Guide

The counter application counts the number of AI-detected objects. The count value can be utilized by defining various actions.

3.1 Counter working process



By setting up a counter application, AIBOX counts objects internally and archives the counting data to internal storage at regular intervals.

The stored data can be retrieved directly from the edge through the API. Edge storage has limitations in areas such as storage period, network configuration, and service delivery performance.

3.2 Counter Setting Example (Occupancy Counting)

Utilize the Occupancy Counting application to count people in real-time not only in stores, but also in buildings, specific areas of buildings, floors, or any other unit.

3.2.1 Counting Method

Occupancy counting operates according to the following methods.

1. Count the number of people entering from all possible entrances to the target space.

2. Count the number of people exiting at all possible exits from the target space.

3. Aggregate and store **the number of people entering – the number of people exiting** for each data collection cycle.

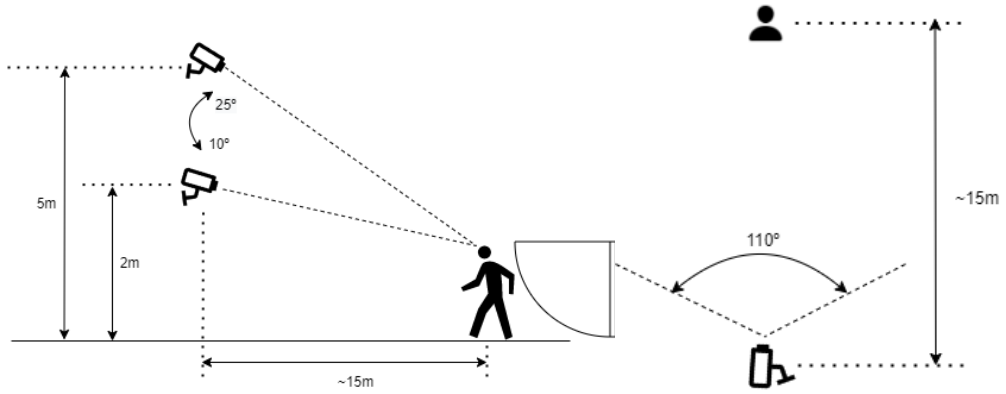
3.2.2 Counting Condition

To ensure that the count value is as accurate as possible, follow these guidelines.

- Compliance with entrance and exit camera installation guide.
- No one enters or leaves the target space other than the designated entrances and exits.
- Specify a daily counter reset time when no one is inside the target space.

3.2.3 Camera Installation Condition

Camera tilt angle	**10º~25º**
Camera installation height	**2m~5m**
Camera horizontal angle	**40º~110º**
Camera resolution	**Over 1280×720, 16:9 Ratio**
FPS frame per second	**6~30**
Transmission bitrate	**2Mbps~10Mbp**
Minimum detection object size	**Horizontal 32px, Vertical 64x**
Distance between camera to object	**~ 15m**



3.2.4 AIBOX Counter Setting

1. To set up counting people in a space, click the **'Explore AI Apps' – 'Occupancy Counting'** in the sidebar navigation menu.

2. Click the 

button to create a new counter in the upper-right corner of the Occupancy Counting list.

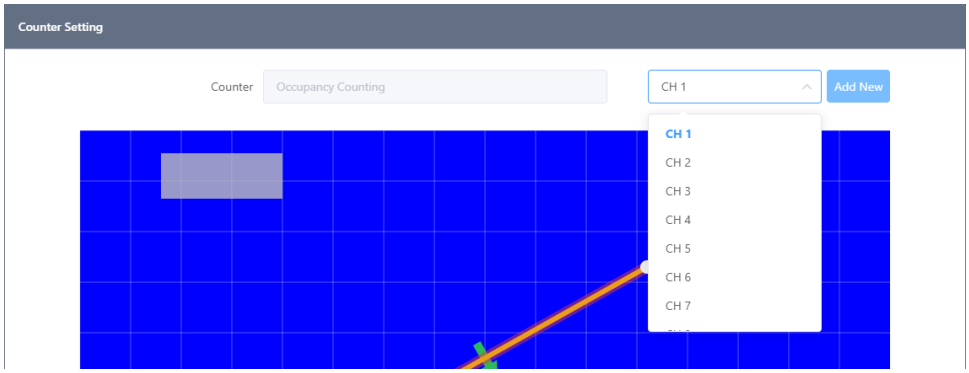
3. Enter the name in the **"Name"** session to distinguish this event action from the other events. Later, you can use the name you enter here to distinguish the event in event history lookups or in actions performed by the action handler.

4. Click the 

button to add the enter/exit zone. If there are multiple entrances and exits, every entrance and exit be added as a counting zone.

3.2.5 Counting Zone Setting

1. Select the video you want to count from the **Select Video dropdown** in the top right corner.



2. The counting area can be set using the functions below.

- Drag the vertex to **move it**
- Click the yellow line to **add a new vertex** at that point
- Right-click the vertex to remove it
- Drag the gray box to move the label position

3. Click the Apply button to save after setting each option. Set the counting zone to every entrance and exit the same as above to count the whole passengers.

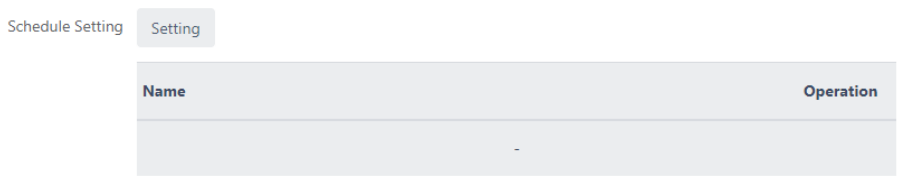
- Zone Name : Enter the name of this zone.
- Counting Zone : Select the direction of people passing by needed to count as an event

3.2.6 Schedule settings (optional)

You can reset the counter at times when there are no people in the target space, such as at night or during non-business hours.

You can set up a wipe schedule as a daily, weekly, or monthly wipe. You can also add multiple wipe schedules.

1. Click the Setting button to set the event action schedule.

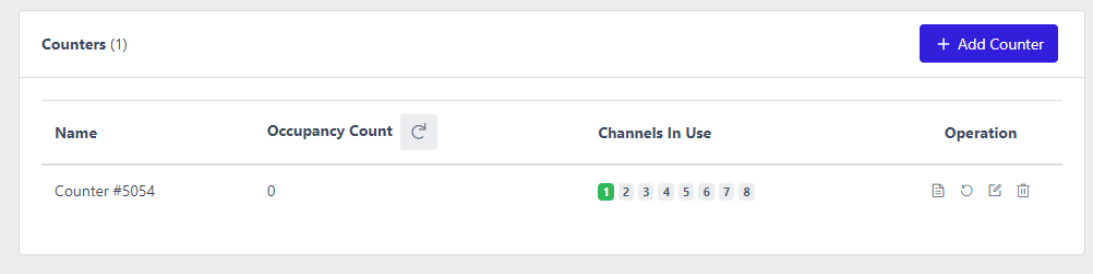


2. Add a schedule to drive action when an event occurs. Please refer to the '**Schedule Setting Guide**' for more information on how to set up a schedule.

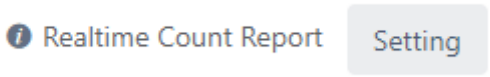
3.2.7 Finishing the setup

1. When you've finished setting up all the entry and exit people counters and reset schedules, click the Submit button at the bottom of the page to submit your in-space people counter settings.

2. If everything is set up correctly, you can see what you've set up in the list of people counters in the space.

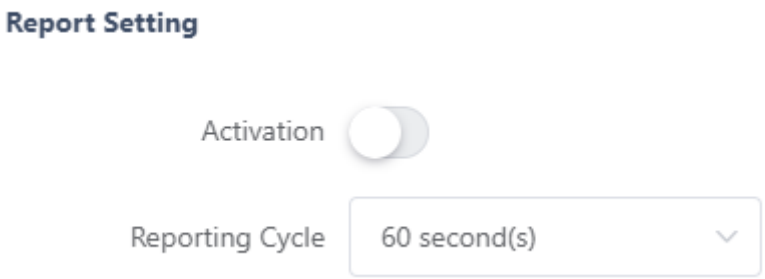


3.2.8 Setting up real-time reporting (optional)



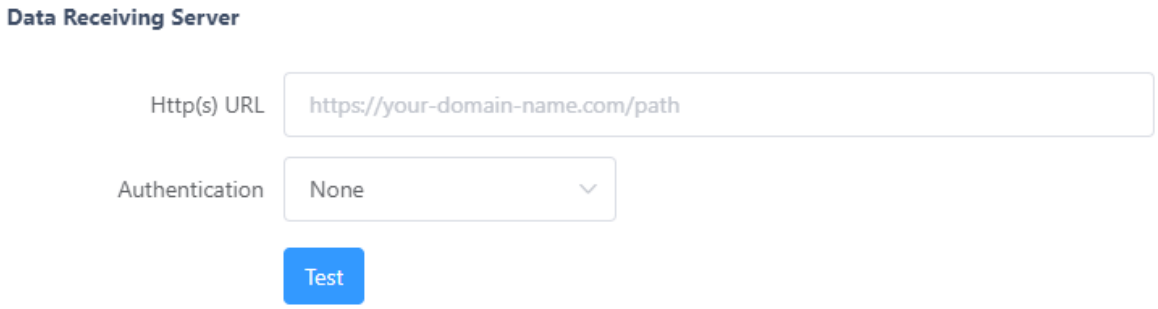
This feature allows you to send count values to a user-configured HTTP server in real time. Not setting it does not affect the behavior of the counter.
Click the "Settings" button to configure the real-time count reporting feature.

3.2.8.1 Reporting setting



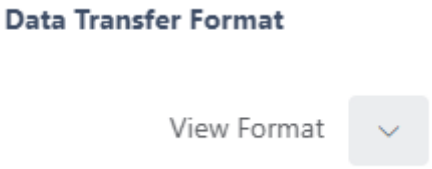
To enable real-time reporting, turn on the switch in the Activation button.
The frequency of real-time reporting is set in the Reporting cycle item.

3.2.8.2 Data Receiving Server



To receive real-time count data, configure the server information.
Add the HTTP or HTTPS server URL and authentication settings if you have authentication capabilities.
The authentication method can be configured as Basic, Digest or Token.
You can use the Test button to check that the device can send data to the server normally once you've set up the data receiving server. When the "Test" button is clicked, data will be sent to the configured HTTP server in the same format as the real time count data of the actual meter.

3.2.8.3 Data Transfer Format

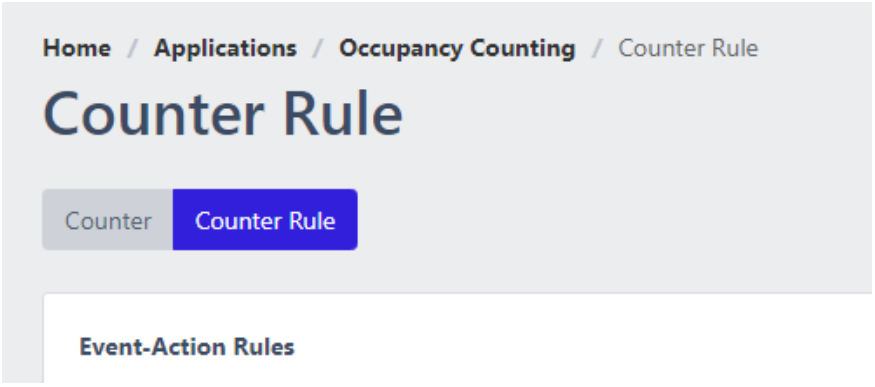


Under Data transfer format, click the button in the View format item to see the live count data transfer protocol information.

3.3 Counter Action Rule Setting Example

You can set events and create action rules based on the counter values of the counters you set.

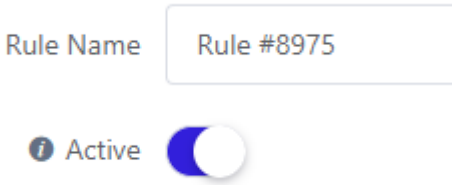
Each counter app includes a separate menu where you can set up rules.



To add a new counter rule, click 

the in the top right corner of the rules list.

3.3.1 Event Action Rule Preferences Setting



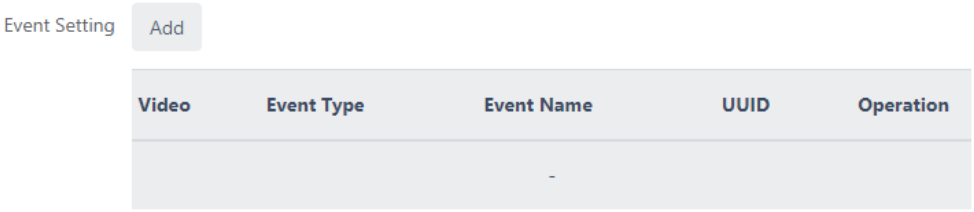
1. Enter a **name** for the rule. A random default value is entered, change this if necessary. You can also identify the rule by the name you enter in the action performed by the action handler.

2. If you want to activate the event action rule upon creation, turn on the **'Active'** switch.

3.3.2 Event setting

1. Click the 

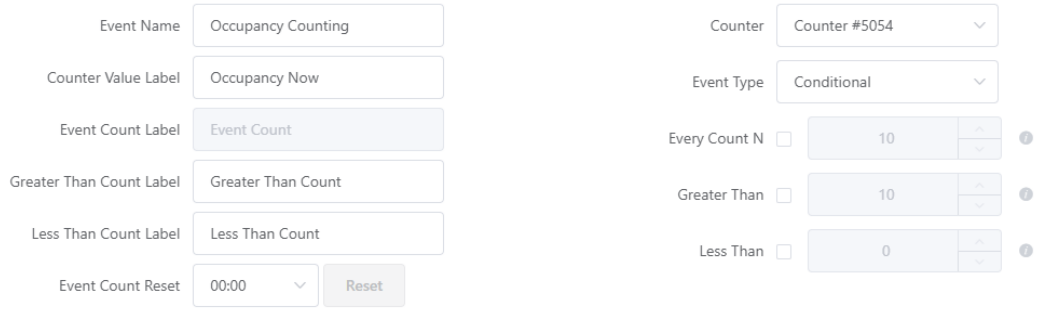
to set the event.



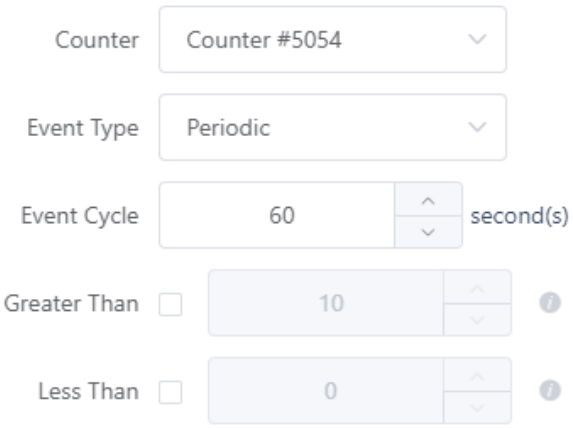
2. Select the channel on which you want the event widget to appear and specify the location of the widget. The channel on which the event occurs will also be set to the channel on which the widget will be displayed.

3. Specify the target counter for the event in Counters. If there are any counters set up in the Counters application, they will be displayed in the list.

- There are two **event types**.
    - Conditional – the event is triggered when the specified counter's value meets a specified condition.
        - Every Count N – Triggers an event when the count value of the counter goes above or below a multiple of the N you set. For example, if N=10, an event is fired when the count value changes from 9 to 10, 19 to 20, or 10 to 9, etc.
    - If you added a range condition, such as greater than/less than, to the condition for every count N – Even if the interval N changes, the event will not occur if the range condition is violated.
        - If the item greater than the setting is greater than the item less than the setting – the event is fired if only one of the two conditions is met. ex) True if "X>10 OR X < 5" if X>10, X<5
        - If the item Greater than the setting is less than the item Less than the setting – the event is fired only when both conditions are satisfied. ex) True if "X>5 AND X<10" if 5<X<10
    - Greater Than – The event is triggered the moment the counter's count value becomes greater than the setting.
    - Less Than – The event is triggered the moment the counter's count value becomes less than the setting.
        - The Greater Than or Less Than events are mutually independent, so there is no condition under which one must be greater or less than the other. The event is triggered when the count value becomes greater or less than the number you set.



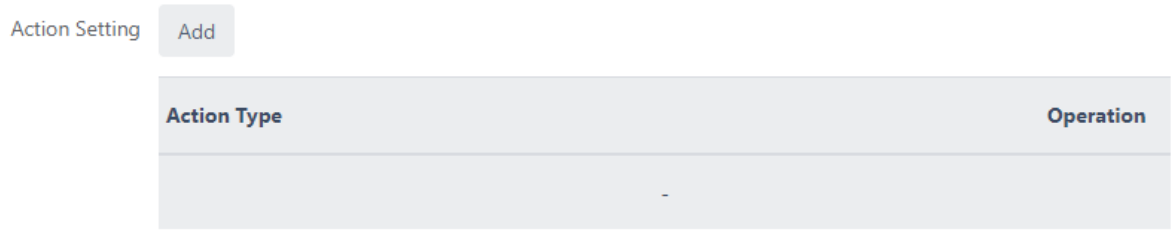
- Periodic – The count event occurs at regular time intervals.
    - Events occur at regular intervals based on the event cycle you set.
    - If you have added a range condition such as greater than/less than setting as a condition every cycle – every count N, the range condition will operate the same way as the setting.



3.3.3 Action Settings

Define the event action to take when the event set occurs in Action Setting.

1. Click the Add button to add a new action item.

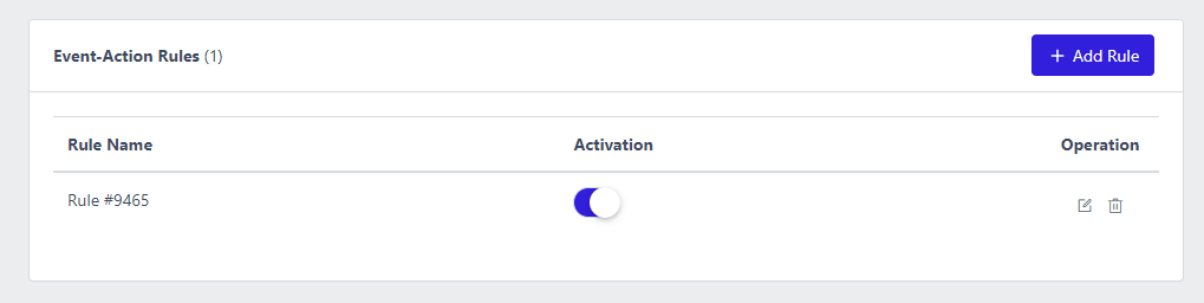


2. Set each action want to perform when an event occurs. Please refer to the '**Action Setting Guide**' for the types of actions supported and how to set them up.

3.3.4 Finish setup

1. Click the Submit button at the very bottom to save intrusion detection event settings after setting up the event, action in the event action rule set page.

2. If everything is set up correctly, you can see the new event in the list on the Intrusion Detection application screen.



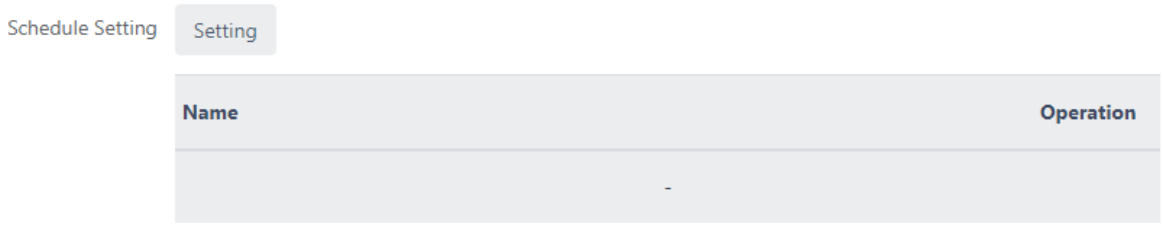
3.3.5 Filter settings (optional)

Schedule and Combined Rule filters can be used to set up event filters to drive actions. The schedule and Combined Rule filter settings described below are not required to configure an action rule, so you only need to set them if necessary.

3.3.5.1 Schedule settings

Set up event action schedules that operate over a period of time to set the time for sending the notification whenever an event occurs.

1. Click the Setting button to set the event action schedule.



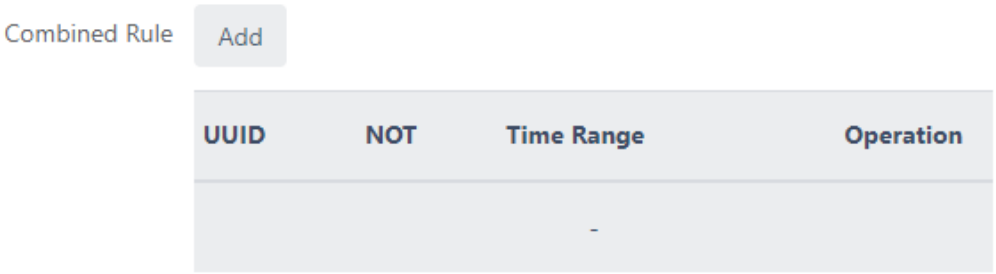
2. Add a schedule to drive action when an event occurs. Please refer to the '**Schedule Setting Guide**' for more information on how to set up a schedule.

3.3.5.2 Combined Rule condition settings

Set compound conditions on event actions to perform more complex forms of event filtering. The following items can be set as compound conditions.

- Rules set in the application in the form of an event action
- Events that make up a rule are set in an application in the form of an event action
- System I/O devices, such as alarm inputs or virtual alarm inputs

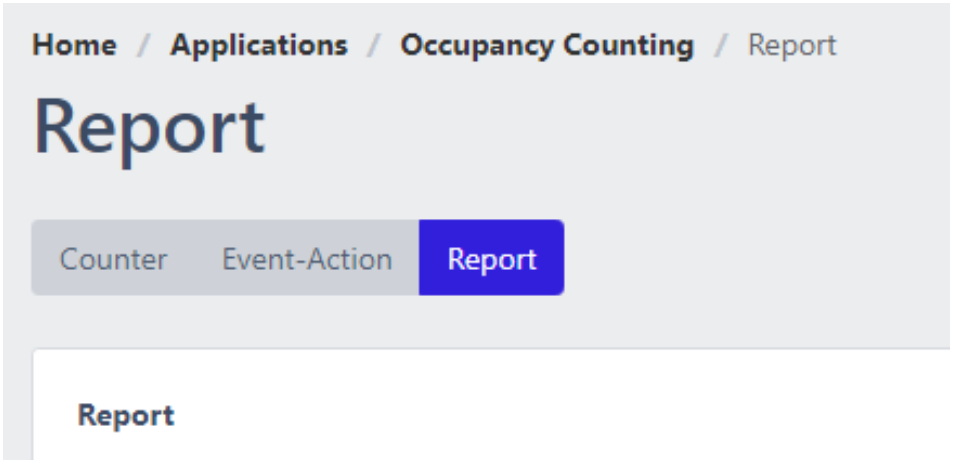
1. Click the Add button to set the combined rule condition.



2. Please refer to the '**Combined Rule Setting Guide**' for more information on setting up.

3.4 Periodic Reporting Setting Example

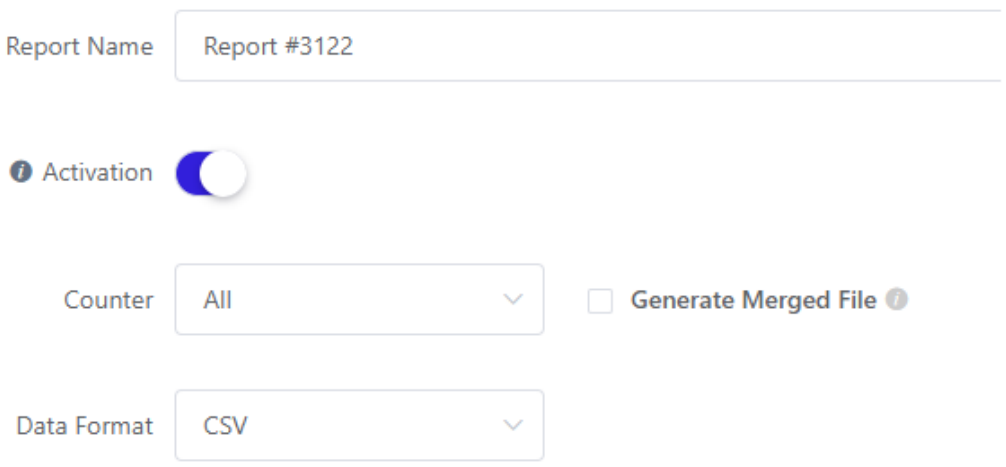
You can periodically report the counts collected by the counters you have set up to storage, such as FTP, email or AWS S3.
Each counter application has a separate menu where you can set up reporting.



To add a new counter rule, click the 

button in the top right corner of the report list.

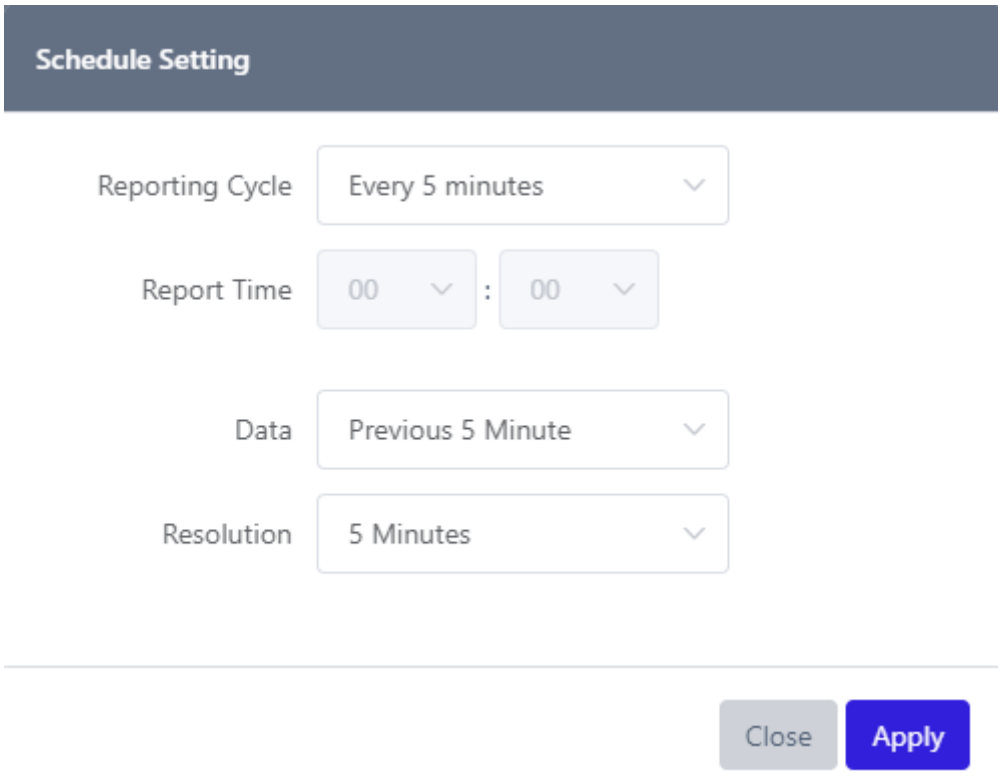
3.4.1 Reporting Preferences Settings



1. **Report Name** : Enter the name to identify this report setting. A random default value is inserted, change this if required.
    - Once you have set a report name, you can use the {{REPORT NAME}} token in the report file name or the directory name in the receiver settings to specify this report name in the report file name or the directory name in the receiver settings.
2. **Activation** : Check the Enable box if you want to enable the report function simultaneously with generation.
3. **Counter** : Set Counters specifies the counters that are included in the report. Counters must be set in advance. The report will include **all counters** that are set when you select **All**.
4. **Data Format :** The Data Format setting specifies the type of reporting data. You can report data in CSV or JSON format.

3.4.2 Schedule Settings

Schedule settings allow you to set reporting frequency, reporting time, reported data scope and reported data units. You can register multiple schedules. Each schedule will send data independently.



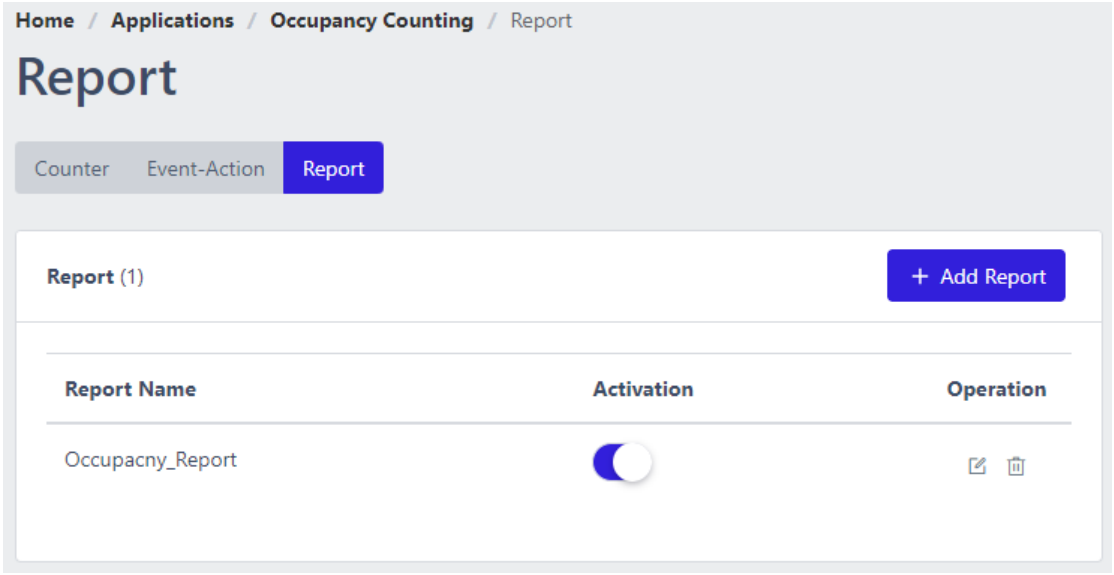
1. **Reporting Cycle** : Set the frequency of data reports.
2. **Report Time** : Set when to report based on reporting cycle.
3. **Data** : Set the scope of reporting data.
4. **Resolution** : Set the units for aggregating report data.

3.4.3 Recipient settings

Recipient settings are similar to action settings in Event action rule settings. You can set a destination for the report to be delivered to.
File transfer protocols are supported such as FTP (SFTP), email and AWS S3.

3.4.4 Finish the setup

Once you've finished setting up your preferences, schedule settings and recipients, click the button at the bottom of the page to submit your reporting settings.
You will see your settings in the list on the Counter Reporting screen if everything is set up correctly.



3.5 Counter Statistics Report Format Guide

Reporting data format

If you've set up reporting, then a statistical report is sent when the next cycle comes around.

Statistical reports are sent as CSV or JSON type data, depending on your settings.

Multiple zones can be set for a single counter. For example, **Counter #1234** can have multiple zones set for it, such as **Zone #1234**, **Zone #1235**, **Zone #1236**, … etc.

Therefore, the format of the statistics report sent is also variable depending on the counter's settings.

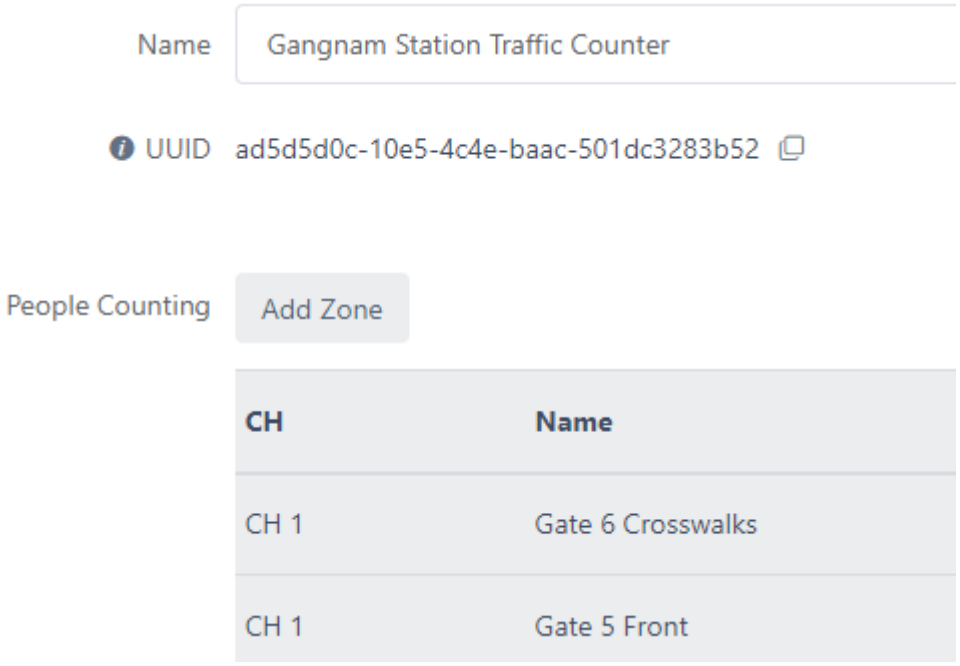
In general, the format of the statistical report will include the following data according to the **counter-zone** hierarchy.

1. Total sum data from the counter
2. Data by each zone

You can see the format of the data being sent referring to an example below.

3.5.1 [People counting] Example of statistical reporting data

If you have the following counters and report set up to periodically receive data from them through reporting settings.



The counter is named **Gangnam Station Traffic Counter**, and it has two counting areas set up: the **Gate 6 Crosswalks**, and **Gate 5 Front**.

By adding reporting settings in the PeopleCounting app, you can receive statistical reports periodically for these counters.

Below is an example of a statistical report set to send in CSV format every 5 minutes.

Example data in CSV format

Example data in JSON format

```
[{
  "timestamp": 1695171300,
  "datetime": "09/20/2023 09:55:00",
  "[cumulative]-Gangnam Station Traffic Counter": 28321,
  "[count]-Gangnam Station Traffic Counter": 230,
  "[A]-Gangnam Station Traffic Counter": 131,
  "[B]-Gangnam Station Traffic Counter": 96,
  "[A]-Gangnam Station Traffic Counter-Gate 6 Crosswalks": 96,
  "[B]-Gangnam Station Traffic Counter-Gate 6 Crosswalks": 38,
  "[A]-Gangnam Station Traffic Counter-Gate 5 Front": 35,
  "[B]-Gangnam Station Traffic Counter-Gate 5 Front": 58
}]
```


Each line contains the following data

Aggregation start time from counters

1. timestamp
    - The Unix Epoch value of when the data started being collected.
2. datetime
    - Date and time values from when the data started being collected. It is set in the format specified in the System-Date and Time setting.

Aggregated statistical data from counters

1. **[cumulative]-counter name** (Ex. [cumulative]-Gangnam Station Traffic Counter)
    - The total sum of the counting data aggregated since this counter was last reset.
    - The cumulative value of the aggregated data from all zone is set in the counter.
    - [cumulative]-counter name = the [cumulative] value of the previous time data + the [count] of the current time data.
    - If there is a count reset schedule, the cumulative value is initialized at that time.
2. **[count]-counter name** (Ex. [count]-Gangnam Station Traffic Counter)
    - The number of aggregates this counter during at that time.
    - Equal to the sum of all counts counted this time in each zone.
3. **[A]-counter name** (Ex. [A]-Gangnam Station Traffic Counter)
    - Sum of all A-direction counts set in this counter
4. **[B]-counter name** (Ex. [B]-Gangnam Station Traffic Counter)
    - Sum of all B-direction counts set in this counter

Statistical data from the individual areas that configure the counter

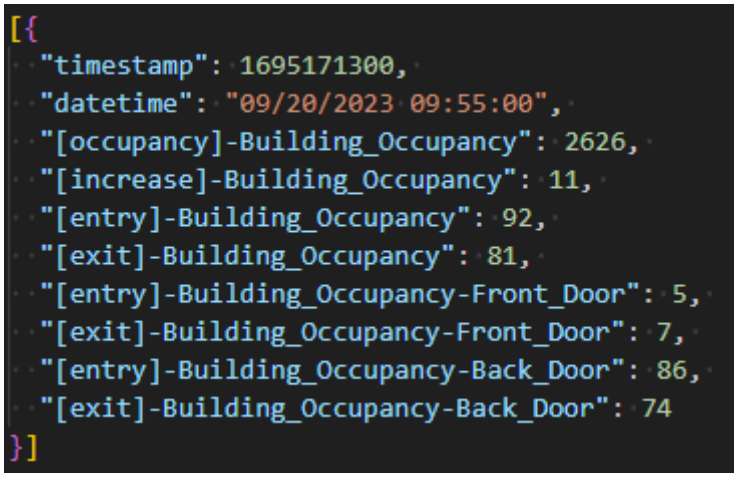
1. [A]-counter name-zone name (Ex. [A]-Gangnam Station Traffic Counter-Gate 6 Crosswalks)
    - Aggregate value in the A direction for the zone
2. [B]-counter name-zone name (Ex. [B]-Gangnam Station Traffic Counter-Gate 6 Crosswalks)
    - Aggregate value in the B direction for the zone

3.5.2 [Vehicle Counting] Example of statistical reporting data

This is the same as the report format in the PeopleCounting app.

3.5.3 [Occupancy] Example of statistical reporting data

Example data in JSON format



```
[{
  "timestamp": 1695171300,
  "datetime": "09/20/2023 09:55:00",
  "[occupancy]-Building_Occupancy": 2626,
  "[increase]-Building_Occupancy": 11,
  "[entry]-Building_Occupancy": 92,
  "[exit]-Building_Occupancy": 81,
  "[entry]-Building_Occupancy-Front_Door": 5,
  "[exit]-Building_Occupancy-Front_Door": 7,
  "[entry]-Building_Occupancy-Back_Door": 86,
  "[exit]-Building_Occupancy-Back_Door": 74
}]
```

Aggregation start time from counters

1. timestamp
    - The Unix Epoch value of when the data started being collected.
2. datetime
    - Date and time values from when the data started being collected. It is set in the format specified in the System-Date and Time setting.

Aggregated statistical data from counters

1. **[occupancy]-counter name** (Ex. [occupancy]-Building_Occupancy)
    - The number of people currently occupied by this counter.
    - [occupancy]-counter name = All entering counting – All exiting counting, since this counter was last reset
2. **[increase]-counter name** (Ex. [increase]-Building_Occupancy)
    - The change in the number of occupied people that this counter has counted at this time.
    - The sum of the (Entry-Exit) values of all zones set in this counter.
3. **[entry]-counter name** (Ex. [entry]-Building_Occupancy)
    - The sum of entering count from all zones that is set in this counter.
4. **[exit]-counter name** (Ex. [exit]-Building_Occupancy)
    - The sum of exiting count from all zones that is set in this counter.

Statistical data from the individual areas that configure the counter

1. [entry]-counter name-zone name (Ex. [entry]-Building_Occupancy-Back_Door)
    - The aggregate number of people entering the zone
2. [exit]-counter name-zone name(Ex. [exit]-Building_Occupancy-Back_Door))
    - The aggregate number of people exiting the zone

Ⅲ. Reduce False Detection Setting

Deep learning object detection cannot be 100% accurate.
There are several tools to reduce false detections and false alarms.
Learn more about these features below and add settings to reduce false detection.

- Object Size Filter
- Object Exclusion Area

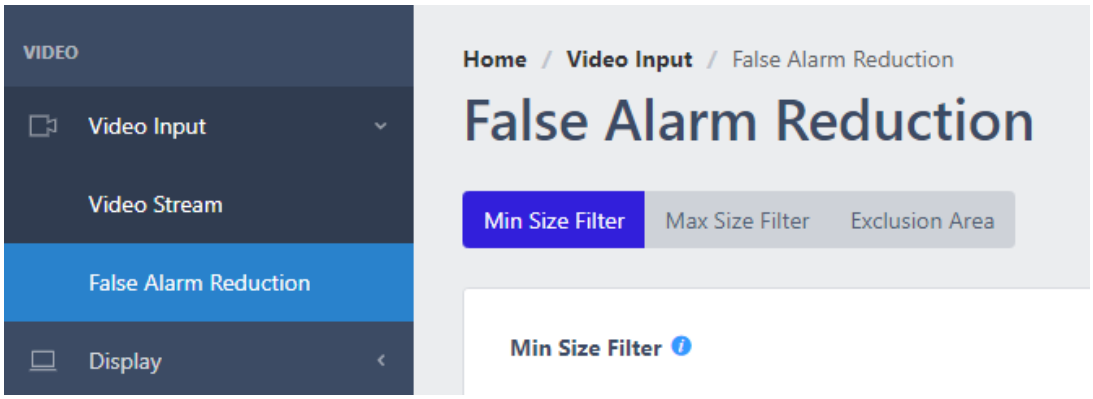
1. Object Size Filter

Within the same field of view, the size of objects of the same type will be approximately constant, or if the field of view is narrow and the distance is close, the size of objects at the top and bottom will increase and decrease at a constant rate and be detected.
These characteristics can be used to exclude detected objects from events if their size is too large or small compared to expectations.

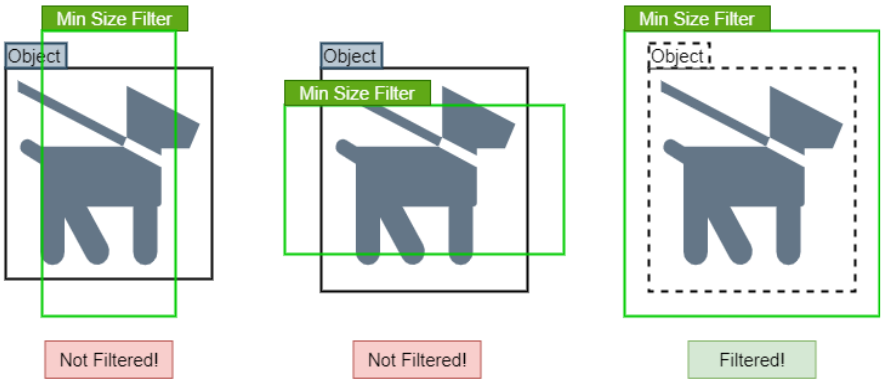
1.1 Object Minimum Size Filter

The Object Minimum Size Filter is a setting that allows a detected object to be recognized as an object only if the size of its bounding box is greater than the size of the box you set.

To access the settings, click Object Size Filter in the sidebar menu and select Min Size Filter in the body area.



1.1.1 How To Filter The Minimum Object Size



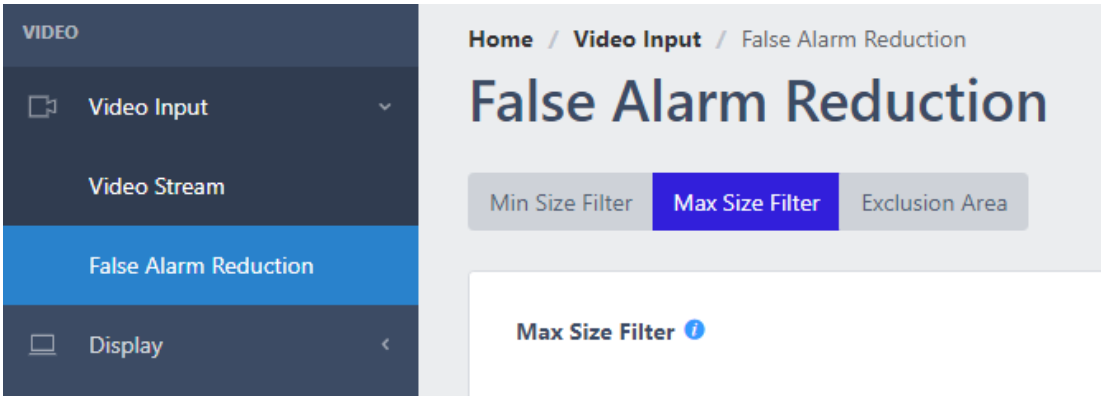
If the bounding box of an object is even larger by one horizontal or vertical dimension than the minimum size filter of the object, it will not be filtered out. Only when the object's bounding box is completely within the minimum size filter will the object be filtered out. See the illustration above to see how the minimum size filter works and which objects are filtered based on the object's bounding box size.

※ Notes
The object minimum size filter is not applied to fire detection.
The object minimum size filter is not applied to fallen detection.

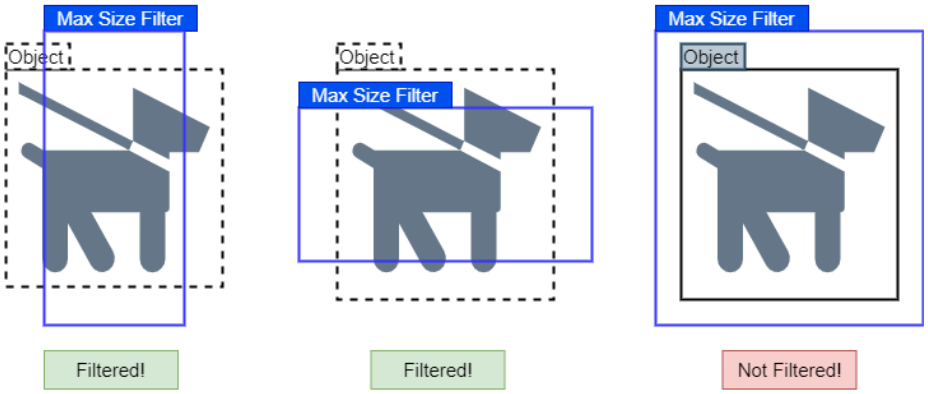
1.2 Object Maximum Size Filter

The Max Size Filter is a setting that only recognizes a detected object as an object if its bounding box is smaller than the specified box size.

To access the settings, click Object Size Filter in the sidebar menu and select Max Size Filter in the body area.



1.2.1 How To Filter The Maximum Object Size

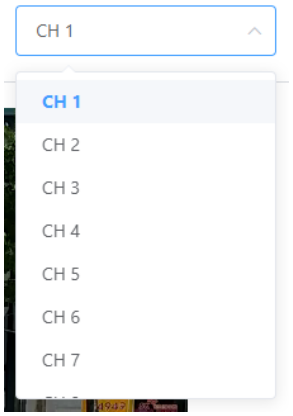


If the bounding box of an object is even larger by one horizontal or vertical dimension than the maximum size filter of the object, it will be filtered out. Only when the object's bounding box is completely within the maximum size filter will the object not be filtered out. See the illustration above to see how the maximum size filter works and which objects are filtered based on the object's bounding box size.

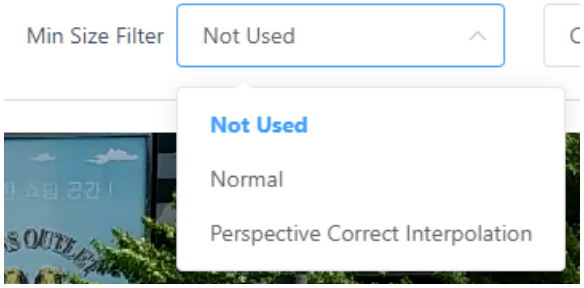
※ Notes
The object maximum size filter is not applied to fire detection.

1.2.2 Filters Set Up

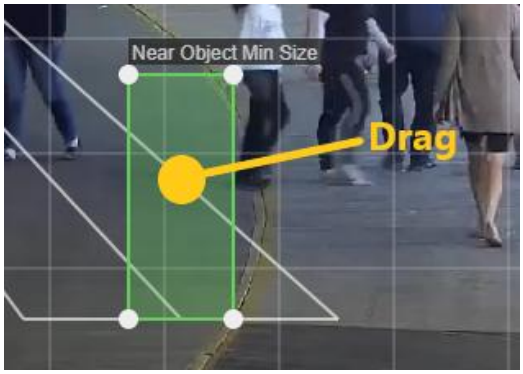
1. Select the channel you want to set the Minimum Size Filter.



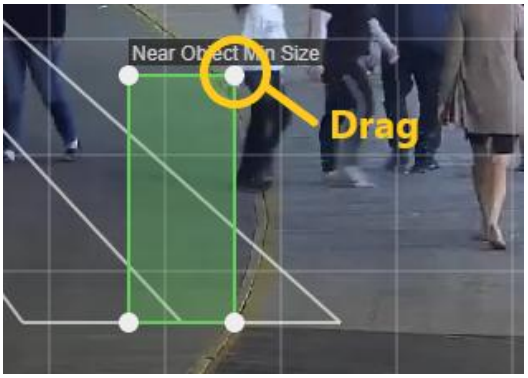
2. Select a Minimum Size Filter type.



3. Drag the filter area to move the filter position.



4. Drag the vertex of the filter box to change the size of the filter.

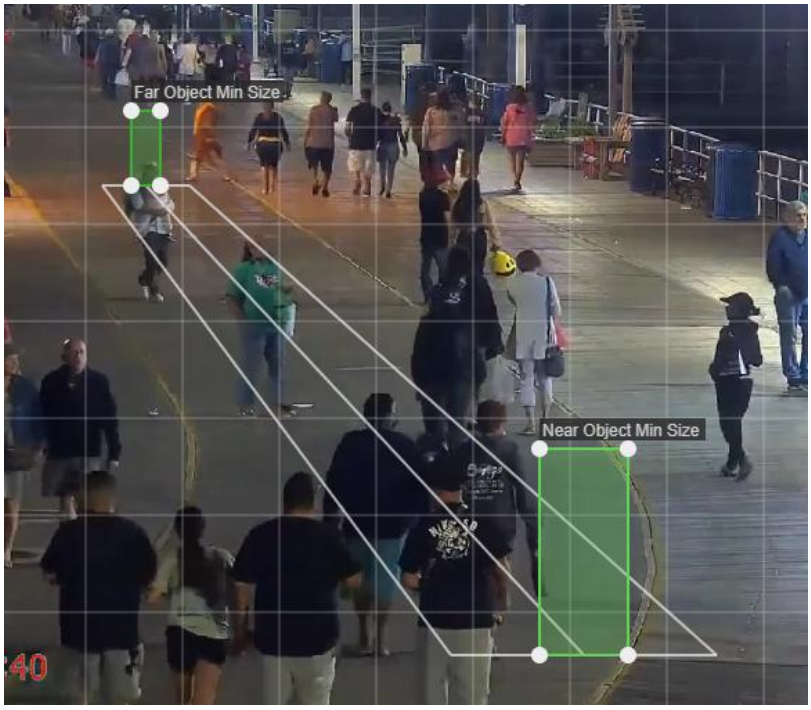


1.2.3 Filter Types

1. Not Used
   1) No use Minimum Size Filter for this channel.

2. Normal
   1) Use a Normal type of Minimum Size Filter.
   2) Typically used when the viewing angle is distant, and the screen area contains objects of approximately similar size.
   3) Set a single box and compares all objects to the size of that box. Objects smaller than the box are filtered out.

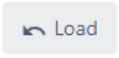
3. Perspective Correct Interpolation
   1) Set two boxes based on perspective.
   2) Set the Near Object Min Size box smaller than the size of objects in the near part of the screen at the bottom.
   3) Set the Far Object Min Size box smaller than the size of objects in the far part of the screen at the top.
   4) A minimum size filter box, calculated as a percentage of the near box and far box, is applied per screen area.
   5) Minimum Size Filter with perspective applied based on where the object appears.



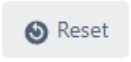
1.2.4 Save, Load, And Reset The Settings

1. Save : Click the 

button at the bottom of the screen to save the position and size information of the filter setting.

2. Load : Click the 

button to load the most recently saved information of the filter that is set on that channel.

3. Reset : Click the 

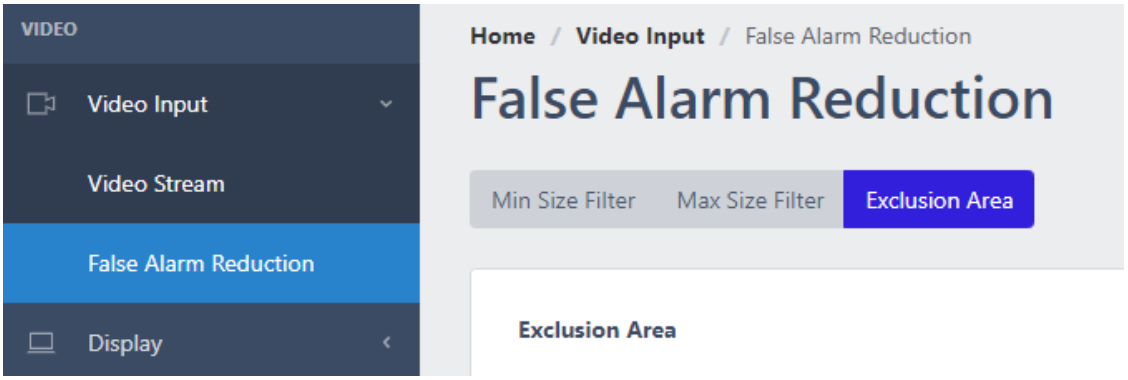
button at the bottom left of the screen to delete and reset the filter settings for that channel.

2. Exclusion Area

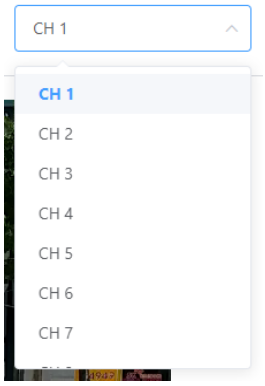
Exclusion zones can be used to filter out the same type of false detection that is consistently occurring in the same location. Objects in the area you added as an exclusion zone will be ignored and will not trigger an event.

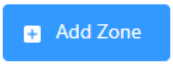
2.1 Exclusion Zone Settings

1. Click the “False Alarm Reduction > Exclusion Area” in the sidebar menu to access the settings menu.



2. Select the channel you want to exclude.

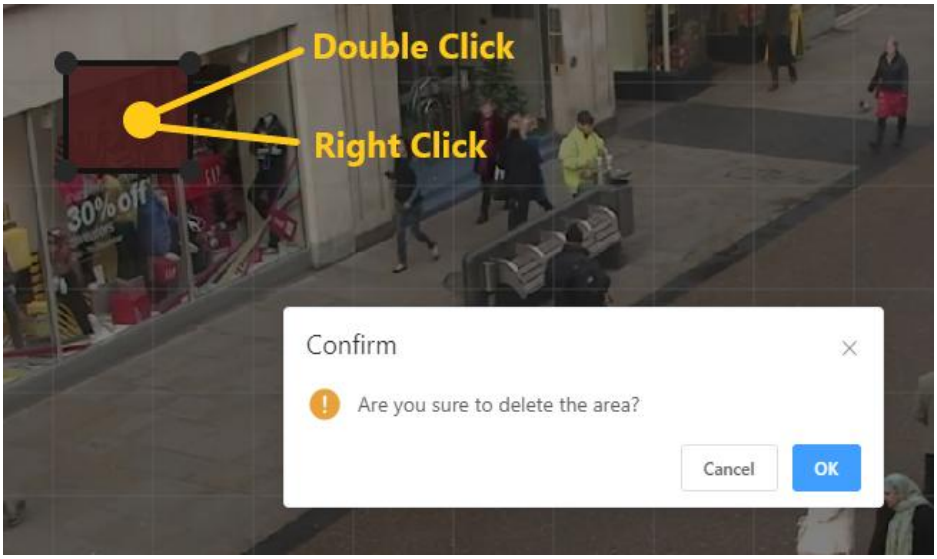


3. Click the  button to create an exclusion zone box. Up to 10 exclusion zones can be set.

4. Drag the exclusion zone to move it.

5. Drag the vertex of the exclusion zone box to change the size of the zone.

6. Double-click or right-click the exclusion zone to delete it.



※Caution
It is recommended that the exclusion area is as small as possible to prevent actual objects from being filtered out by the exclusion area settings.
Even if the exclusion zone does not cover the entire object, the object is excluded as long as its center is within the exclusion zone.

2.2 Save, Load, And Reset The Settings

1. Save : Click the Save button at the bottom of the screen to save the position and size information of the filter setting.

2. Load : Click the Load button to load the most recently saved information of the filter that is set on that channel.

3. Reset : Click the Reset button at the bottom left of the screen to delete and reset the filter settings for that channel.

Arm/Disarm Setting Guide

1. Arm/Disarm overview

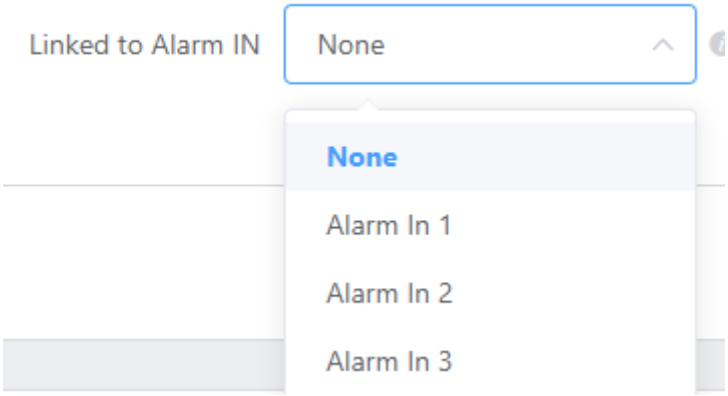
In the Disarm settings, you can set the disarm for whether the action is triggered when an event occurs.

Arm/Disarm Overview
In a disarmed state, no actions are triggered when an event occurs. In addition to the settings that are enabled by default on **webpage**, you can change the state by entering **alarm input**, **schedule**, etc.

You can change the global disarm status of the device via Arm/Disarm Arm button in the top header.

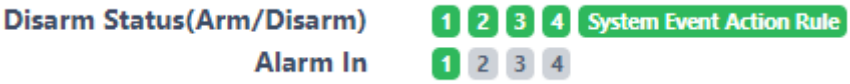
If you checked the Arm activation button even when disarmed in the Arm/Disarm rule settings, the action will run.

2. Global Disarm



The global disarm status is synchronized with the status of the selected alarm input.
When linked to an alarm input, the disarm status cannot be changed via the webpage and API.

3. Arm/Disarm instant settings

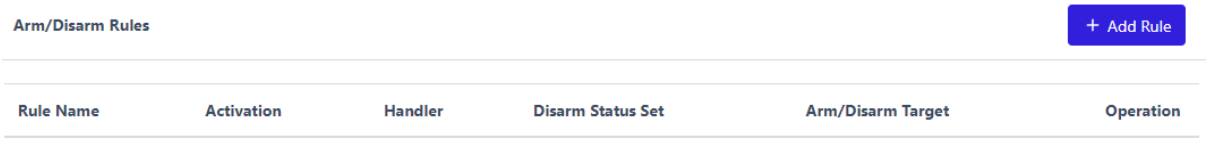


※ Disarm Configuration

- Global: t can be configured in the top header of the UI, allowing you to control the operation of all device actions. This setting takes priority over per-channel settings and system action disarm rules
- All: You can configure the Arm or Disarm operation of all channels and specified actions..
- Per channel: You can configure the operation of all channels and the specified actions
- System Event Action Rule: You can set whether an action set in a system event/action rule is triggered or not.

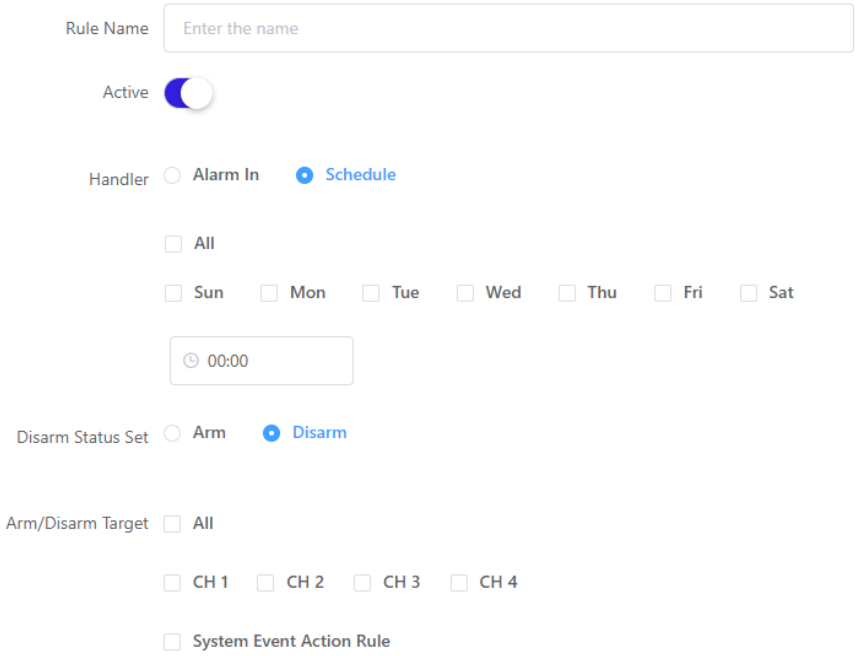
In the Arm/Disarm instant settings, you can set the status of all, per-channel, and system event action rule individually via the buttons. In Arm/Disarm Instant Settings.
If the status of the global disarm is set to disarmed, the event action will not run regardless of the per-channel armed status.

4. Arm/Disarm rules



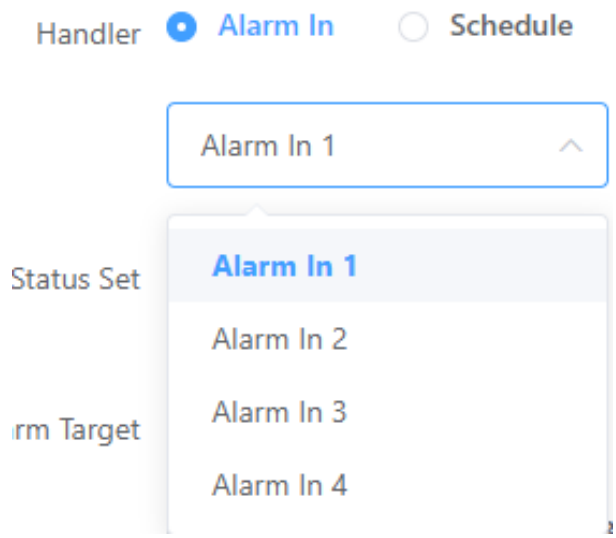
On the Arm/Disarm Settings screen, you can add a rule by clicking 

button.



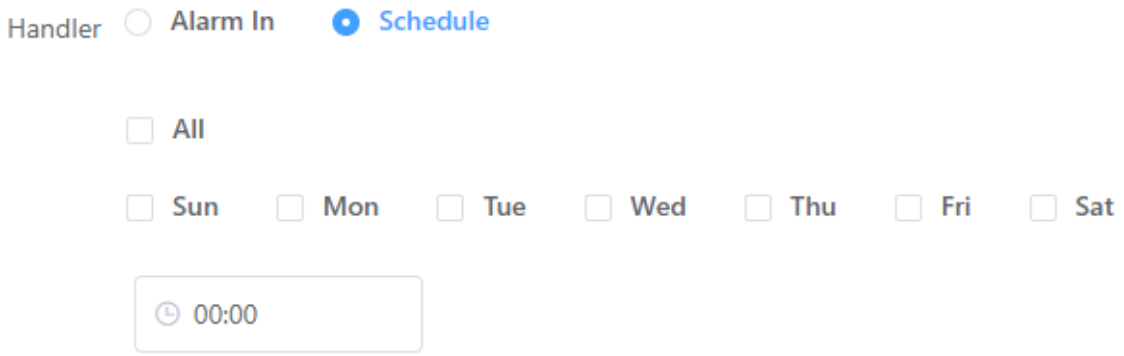
1. Enter a **rule name** to distinguish of rule.
2. The **activate button** sets the rule's activation status.
3. **The handler** specifies whether this rule is for alarm input or schedule.
4. **Disarm state set** configures the arm/disarm state when the rule triggers.
5. **Arm/Disarm target** chooses the entities affected by the rule.

Alarm Input



You can set up a rule by specifying the alarm input to use.

Schedule



You can set a schedule to change disarm status.
You can set a schedule by setting a target day and specifying a time. For example, you can set a rule to disarm every Saturday at 00:00.
Was this helpful?

Generic Event Setting Guide

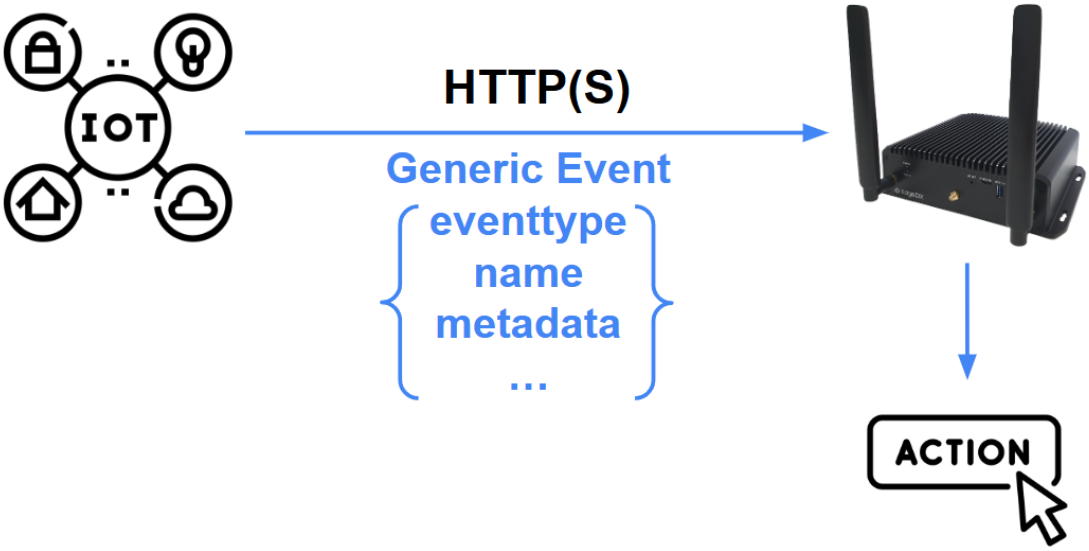
1. Introduction

1.1 Prerequisites

- AIBOX FW version 103708 or higher.

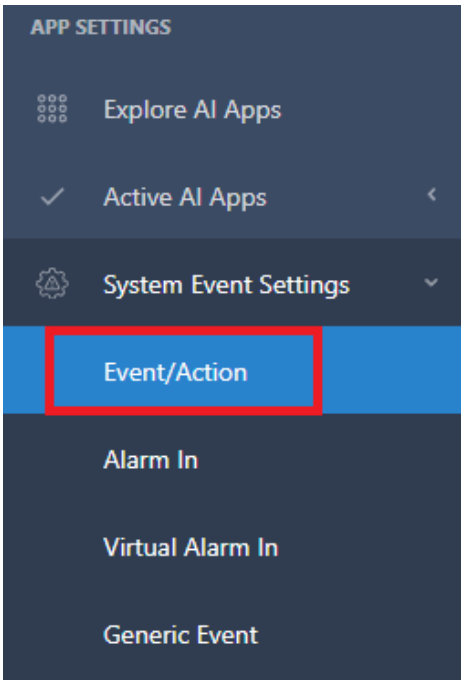
1.2 Learn about integration architecture

The Generic Event allows events to be sent by calling the API using the HTTP(S) protocol from an external source. Since the HTTP protocol is used, account information needs to be entered. For security reasons, it is recommended to add a new API-specific account instead of using the admin account. When the event is triggered, it can be mapped to various actions. Unlike Virtual Alarm In, when sending the event, multiple details can be transmitted through the query string, and there is the advantage of being able to send metadata freely in JSON format.

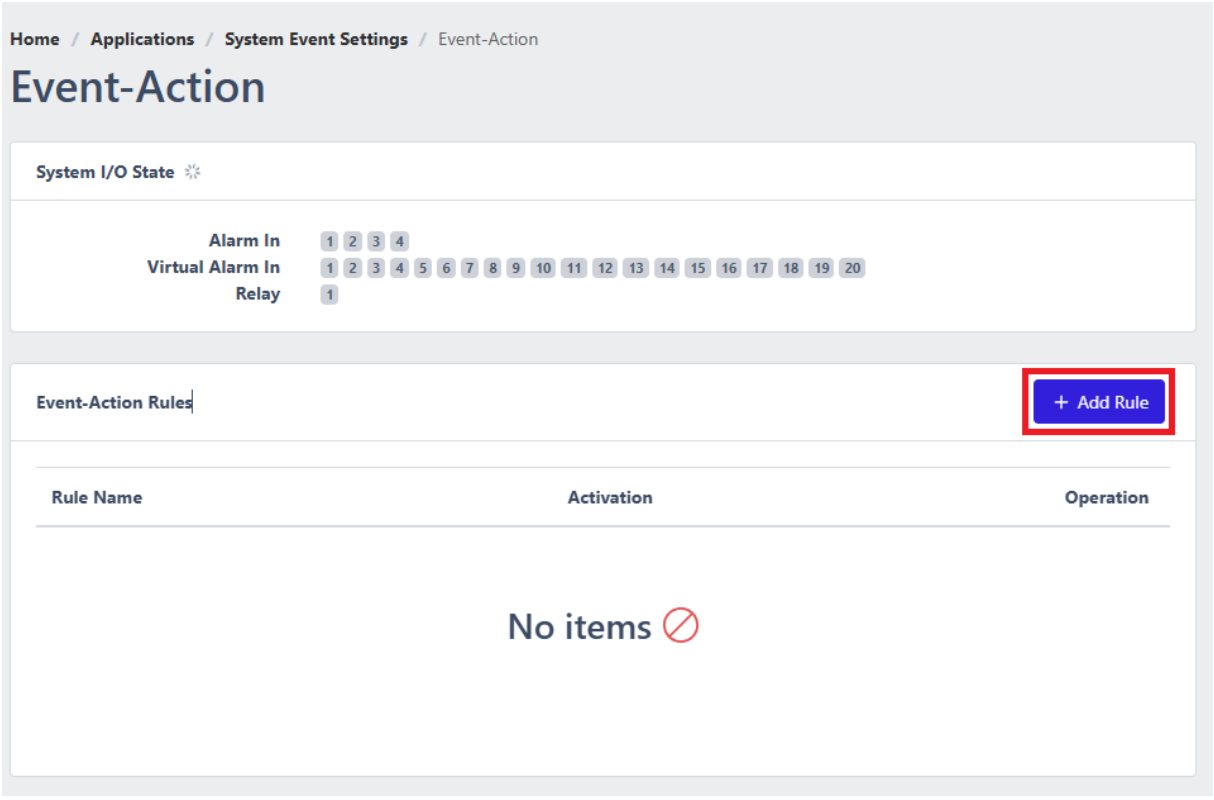

IOT
HTTP(S)
Generic Event
eventtype
name
metadata
...
ACTION

2. Configuration
To use the Generic Event in the AIBOX, the following settings must be configured.

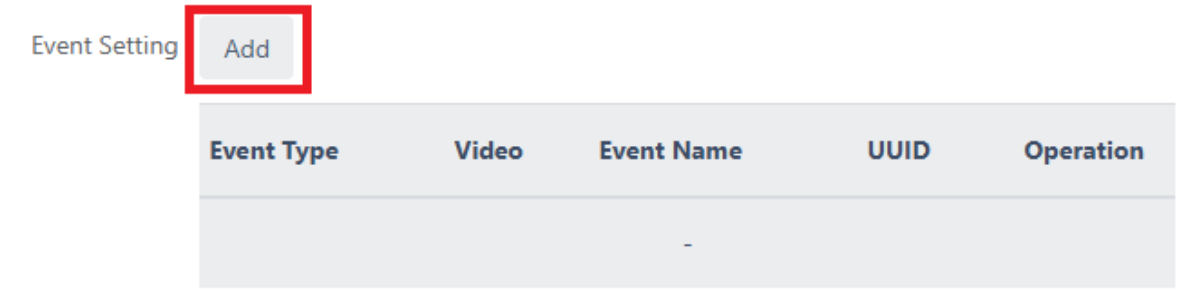
2.1 Event Setting
The method to use Generic Event in the AIBOX is as follows.
Access the AIBOX and click on “APP SETTINGS” > “System Event Settings” > “Event/Action” menu on the left sidebar.



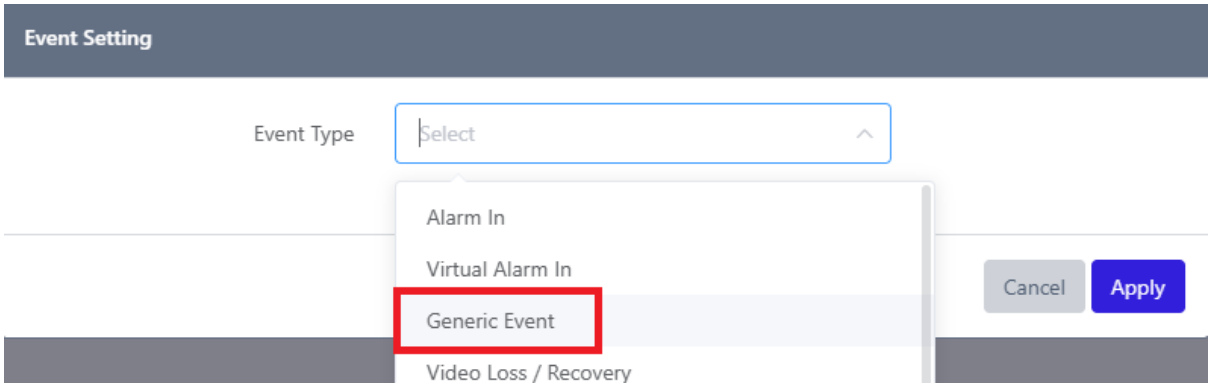
Click the “Add Rule” button.



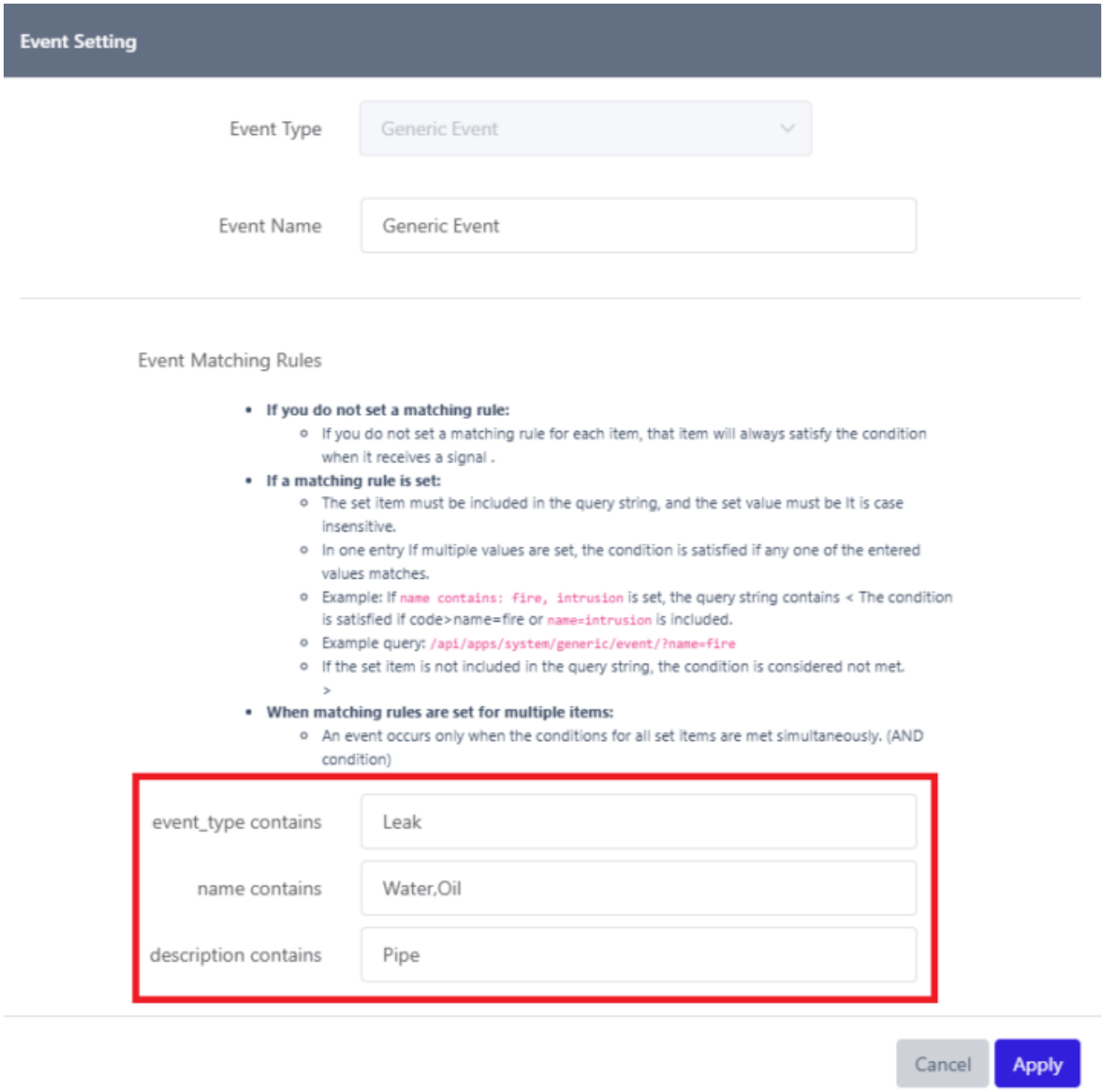
Click on “Event Setting Add.”



Select “Generic Event” from the Event Type.



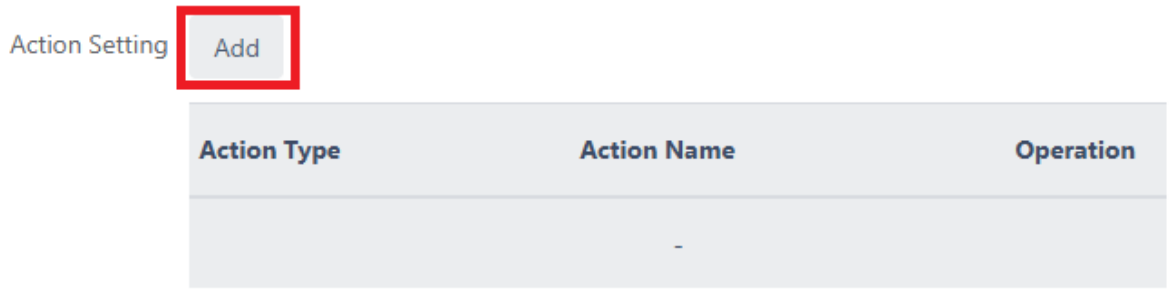
Enter the event_type, name, and description. The Generic Event sends the event via query parameters, and if any of the entered values match, the event will be triggered. Once the settings are complete, click the “Apply” button.
All values entered in the input fields are required. However, if there are words separated by commas (e.g., Leak, Water, Pipe), the action will trigger if any one of the entered words is included.
(For example, the value could be “Leak, **Water**, Pipe” or “Leak, **Oil**, Pipe”)



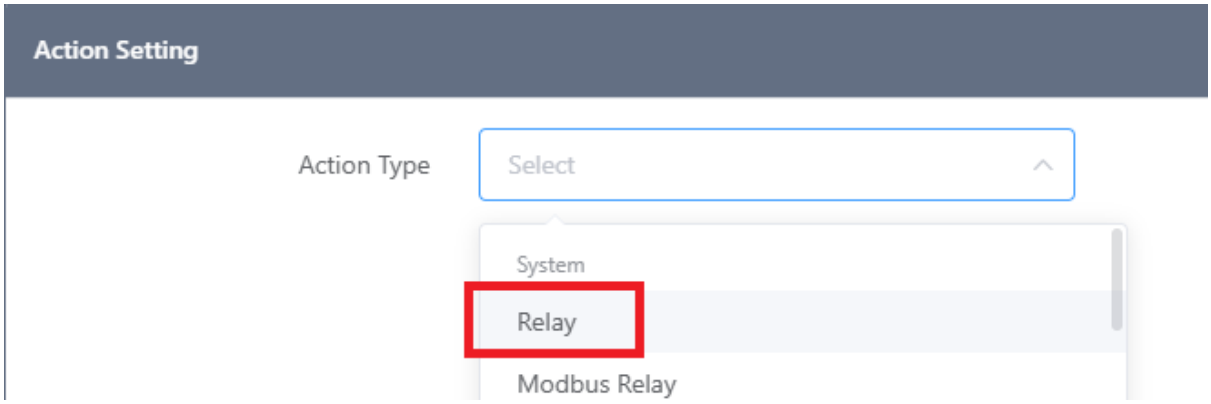
2.2 Action Setting

Once the Generic Event setup is complete, you need to configure the action that will occur when the event is triggered. The following explains the process, and this guide document uses Relay as an example.

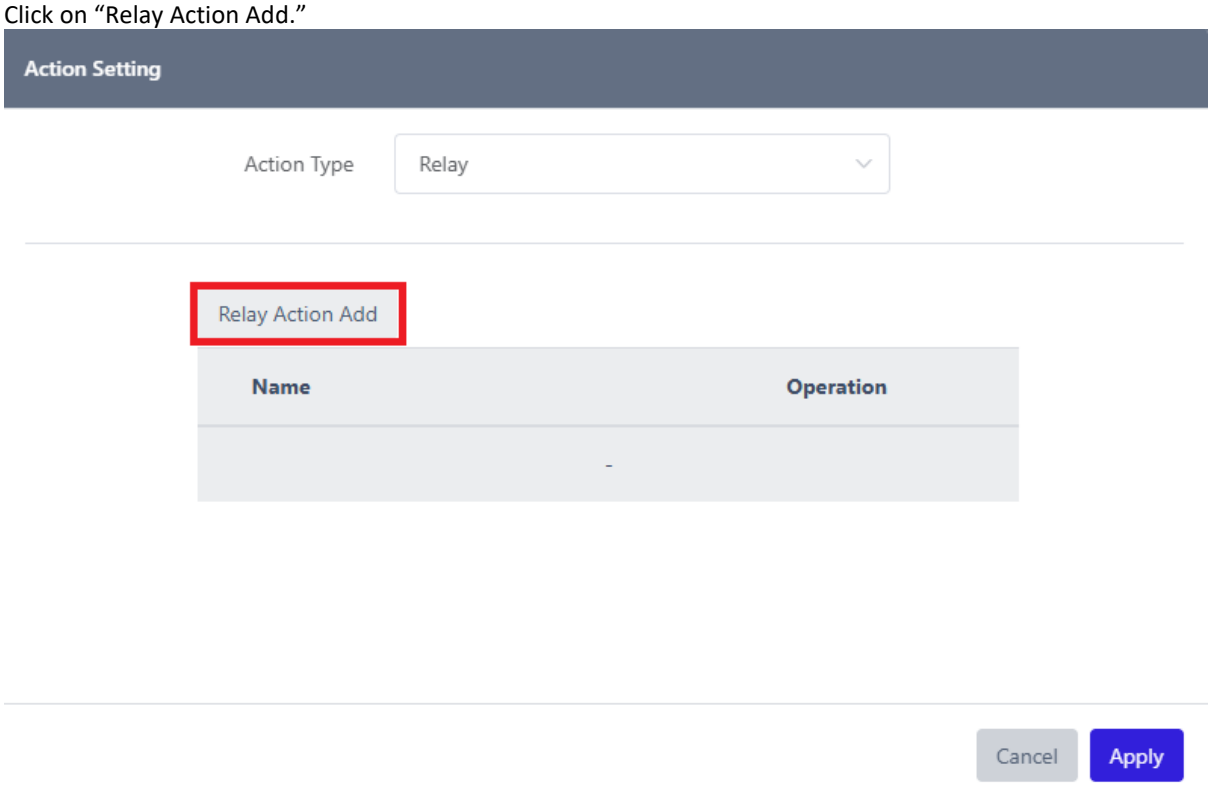
Click the “Action Setting Add” button.



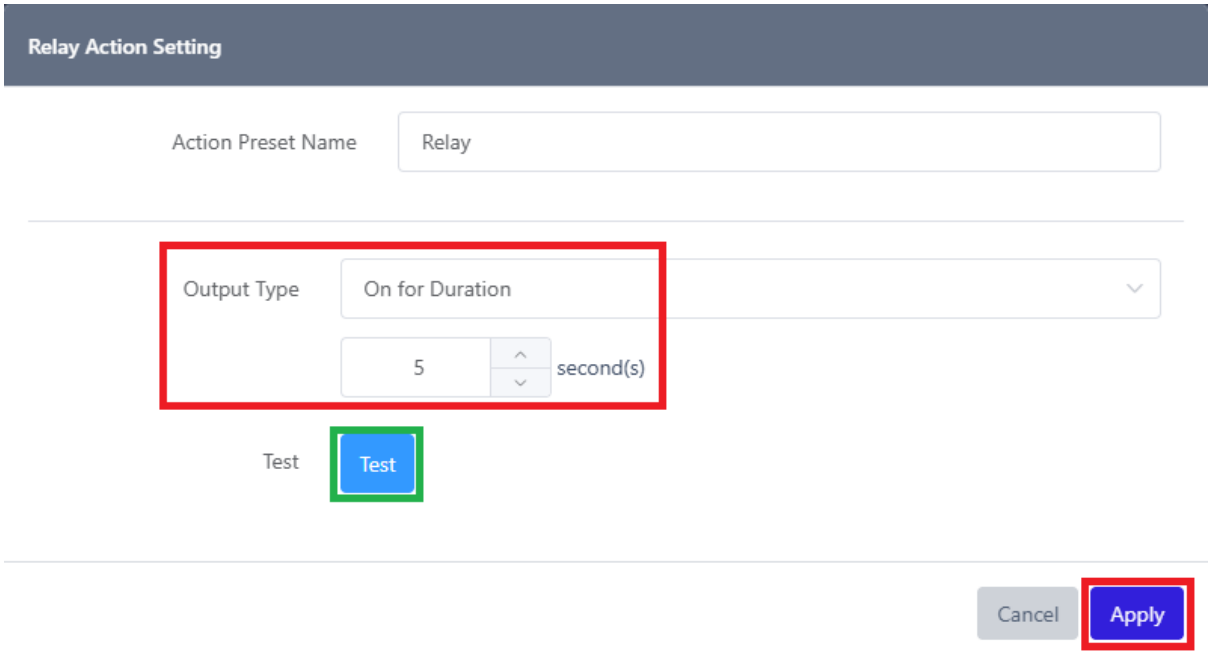
Click on “Relay.”



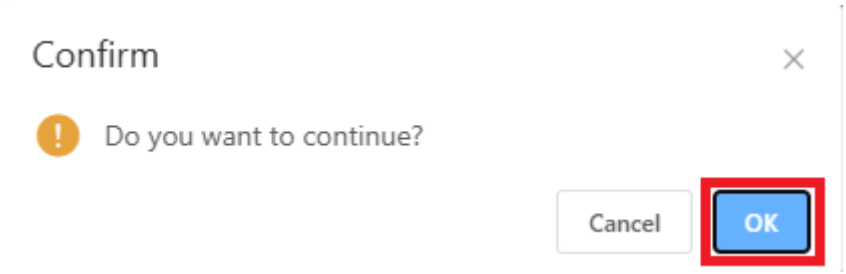
Click on “Relay Action Add.”



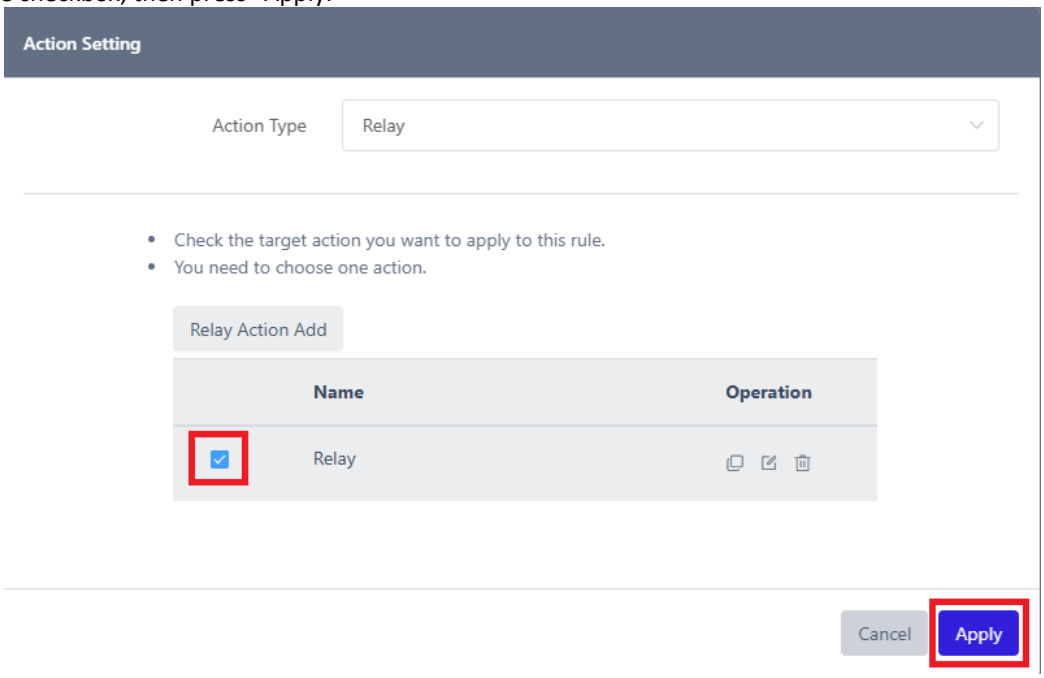
Set the desired Output Type. You can test it by pressing the “Test” button. Once the settings are complete, click the “Apply” button.



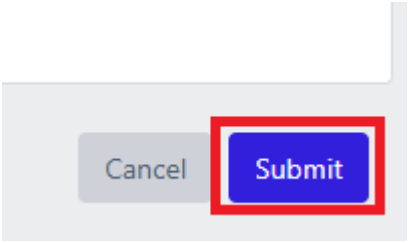
Tip. When the relay is turned on and off, you will hear a clicking sound from the AIBOX.
Click “OK.”



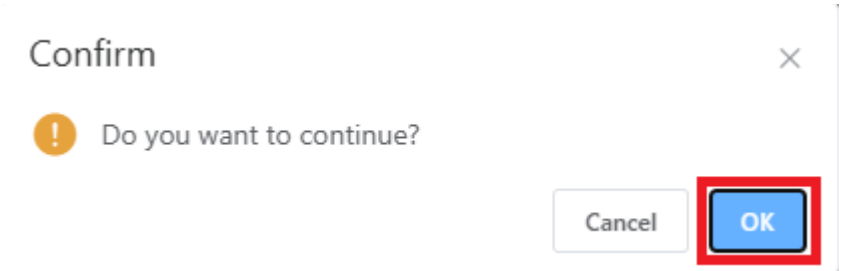
Click the checkbox, then press “Apply.”



Click the “Submit” button at the bottom right of the settings page.

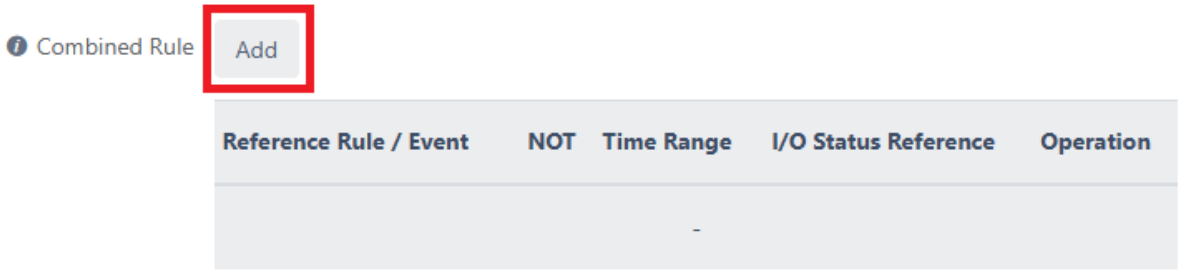


Click “OK.”

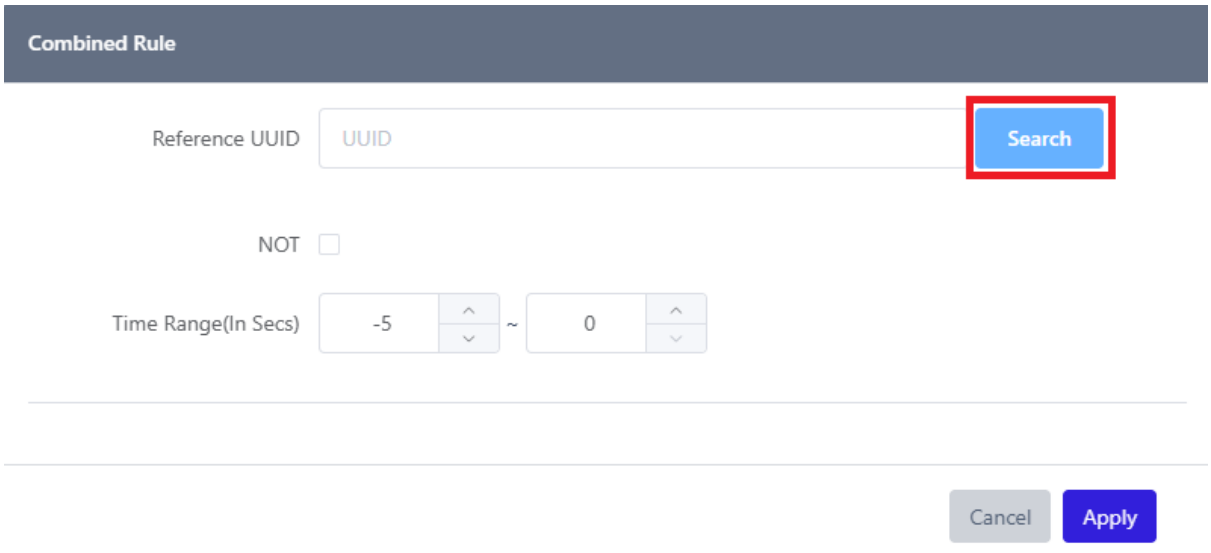


2.3 Combined Rule Setting

If the action setting is complete, you can additionally set up a Combined Rule. Please follow the steps below.
Click the “Combined Rule Add” button.

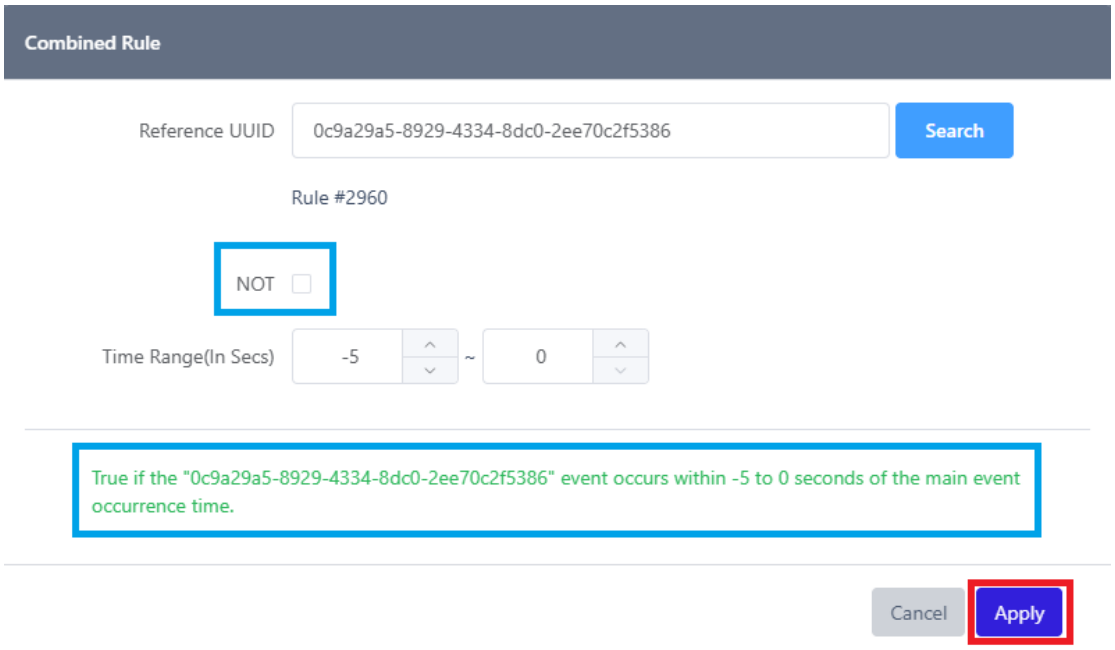


Click the “Search” button.

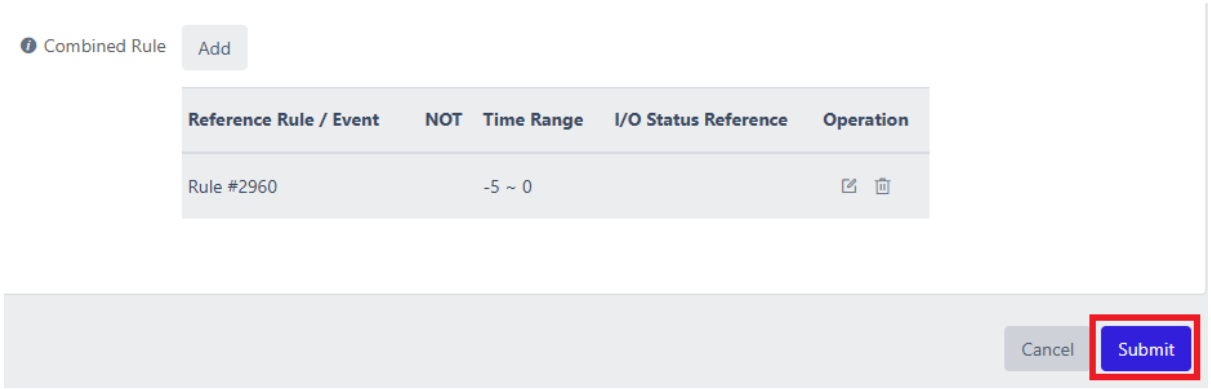


Select the UUID to be combined.

Read the instructions, set the desired values, and then click the “Apply” button.



Note. On the other hand, you can also combine the Generic Event with other pre-existing app events (e.g., Intrusion).
Confirm that the settings are complete and click the “Submit” button.

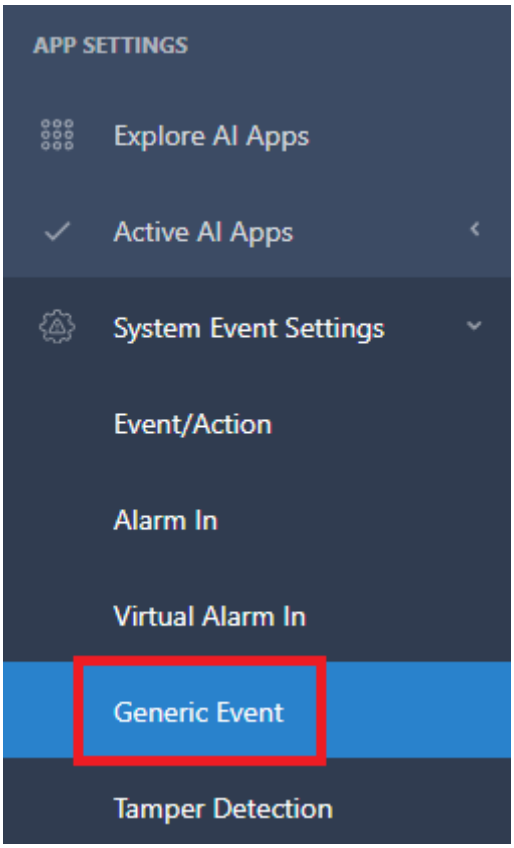


3. Demo

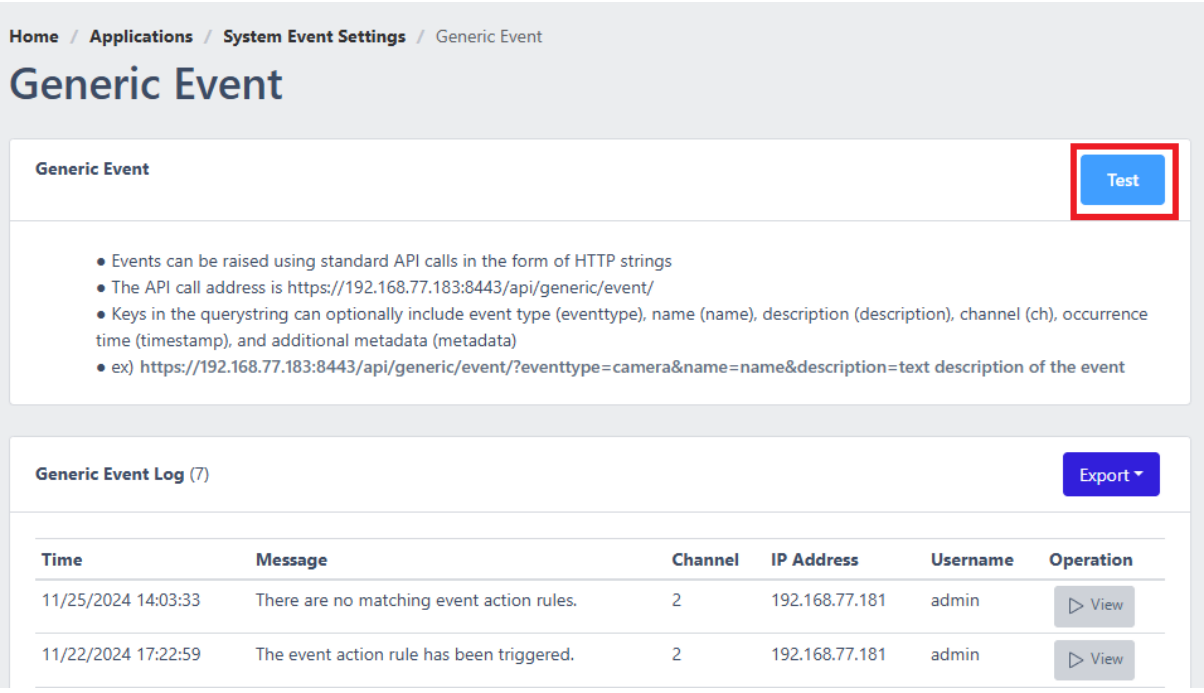
Now, you can check if the Event/Action is properly mapped.

3.1 Testing using the AIBOX

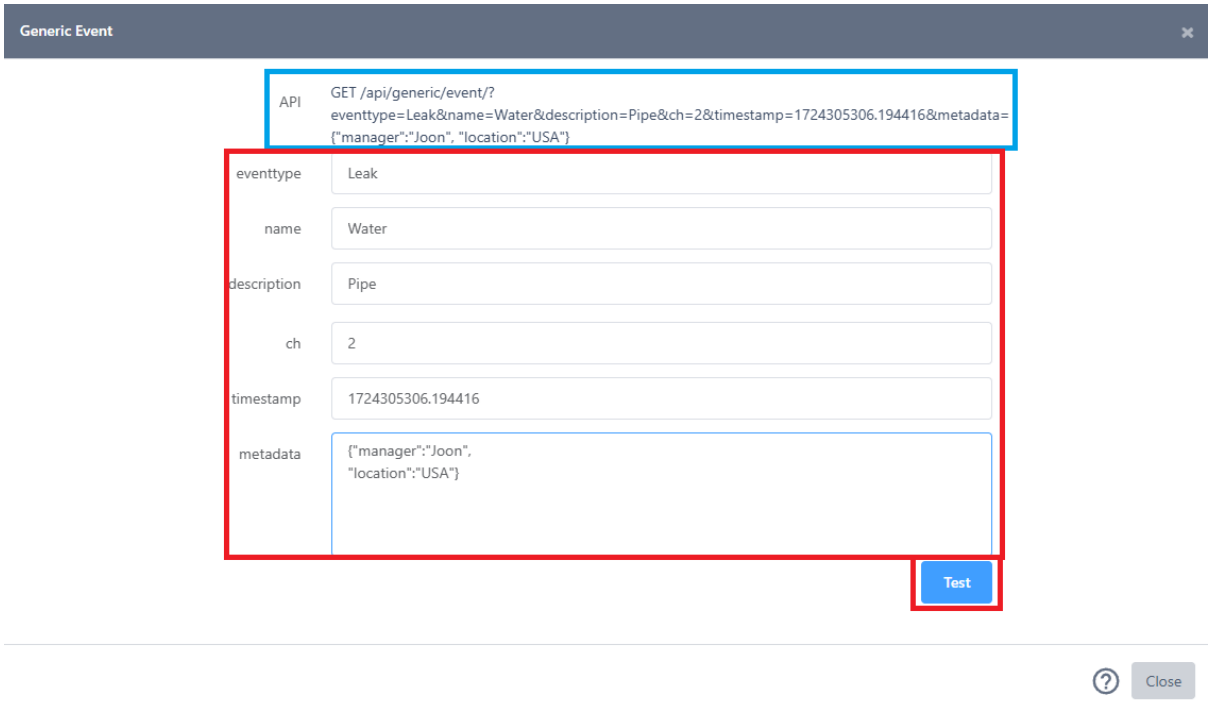
Access the AIBOX webpage and click on “Generic Event” under “System Event Settings” in the “APP SETTINGS” menu on the left sidebar.



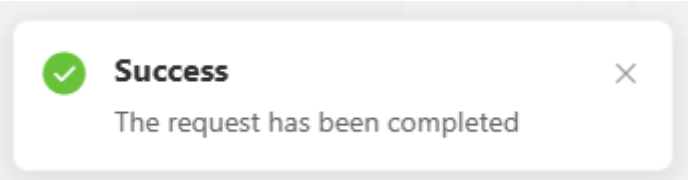
Click the “Test” button.



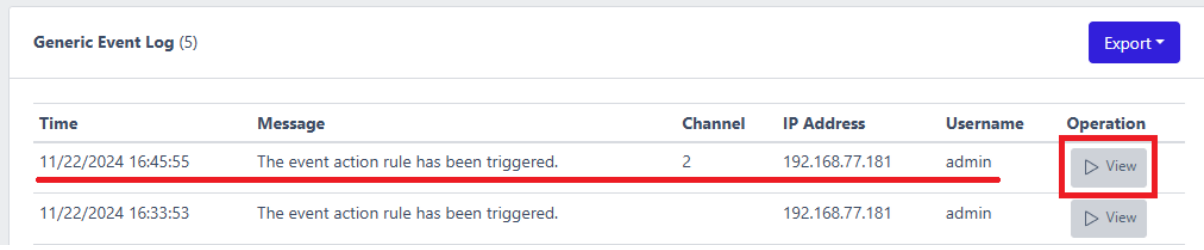
Fill in the properties of the event to be requested for testing, then click the “Test” button. The final API request will be displayed inside the green box.



If the test is successful, a pop-up like the one below will appear, and the relay will click.

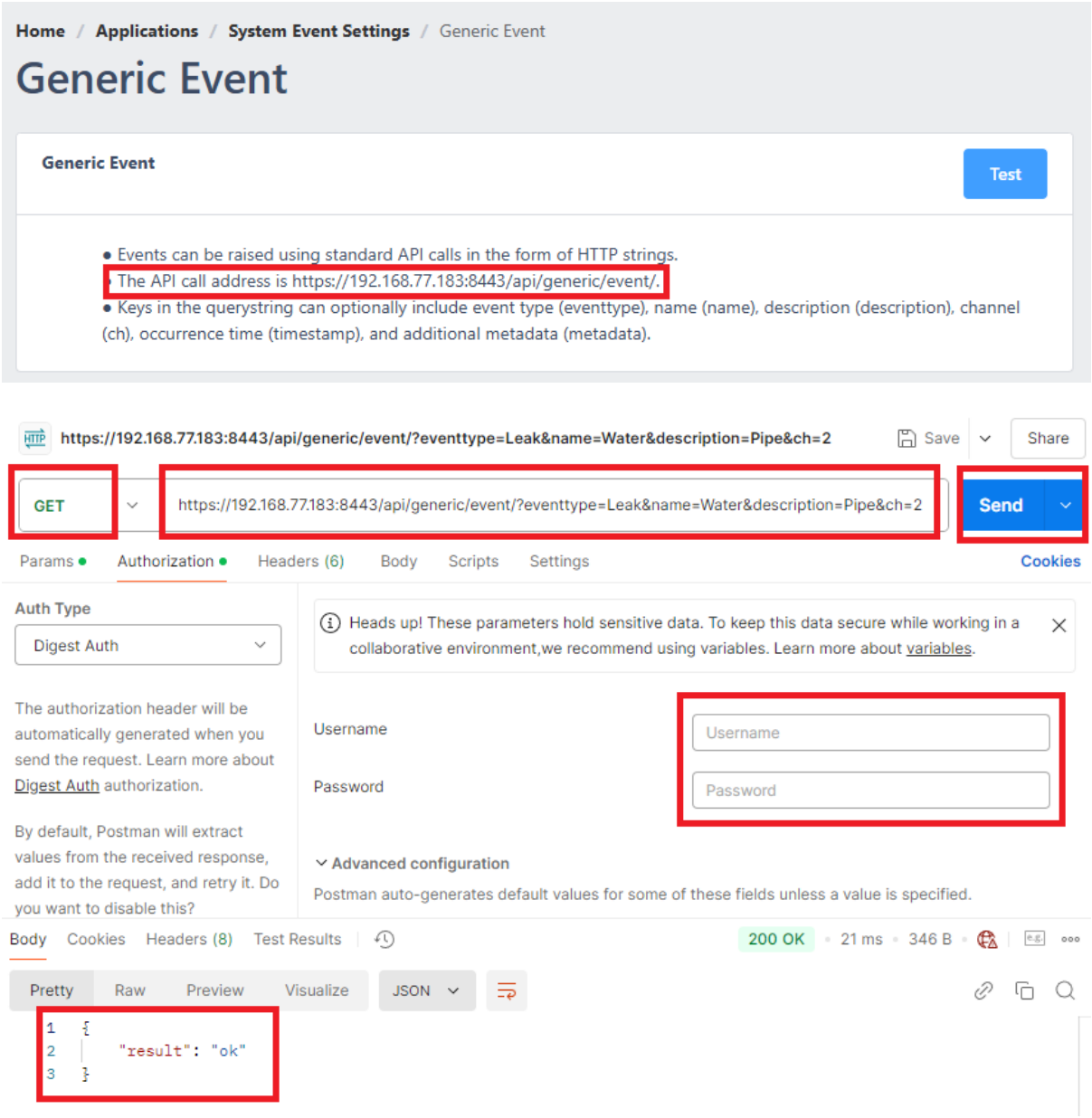


You can view the events that occurred in the list, and by clicking “View,” you can see the details.



3.2 Testing using Postman

Open Postman and add the account information under Authorization. Append the query string to the specified endpoint to make the request.
(e.g., /api/generic/event/?eventtype=Leak&name=Water&description=Pipe&ch=2)
If the request is successful, an “OK” response will be returned, and the relay will be triggered.



IV. Action setting guide

Utilizing Event Meta Tokens & Creating Action Message Guide

Action handlers that use the network can send messages using various event meta-information, such as the **event name** and the **event occurring time**.

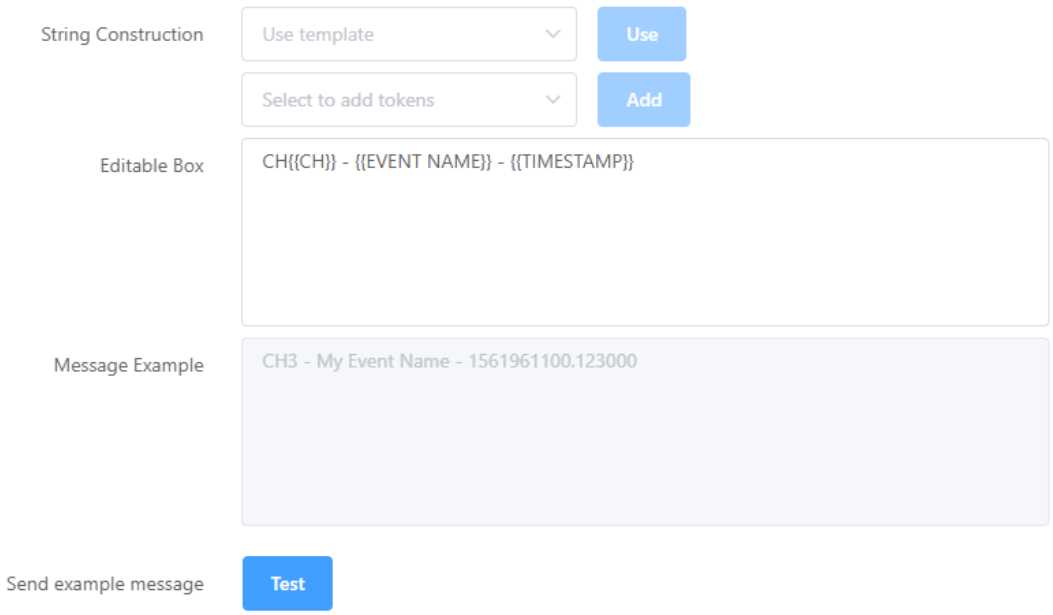
When you set up an action handler of the type that sends a message from a device, the action message you want to send is configured in a format that you edit yourself.

By using the various event meta tokens provided when editing an action message, you can easily add dynamic event meta information to your action message.

This approach to action handlers allows users to write and use protocols with a high degree of freedom, depending on the protocols of the target device or server you want to interact with, without requiring additional development.

Edit Action Message UI Components

The Edit Action Message UI consists of a **template settings control, a token settings control, an edit box, an example box,** and **a test button**.



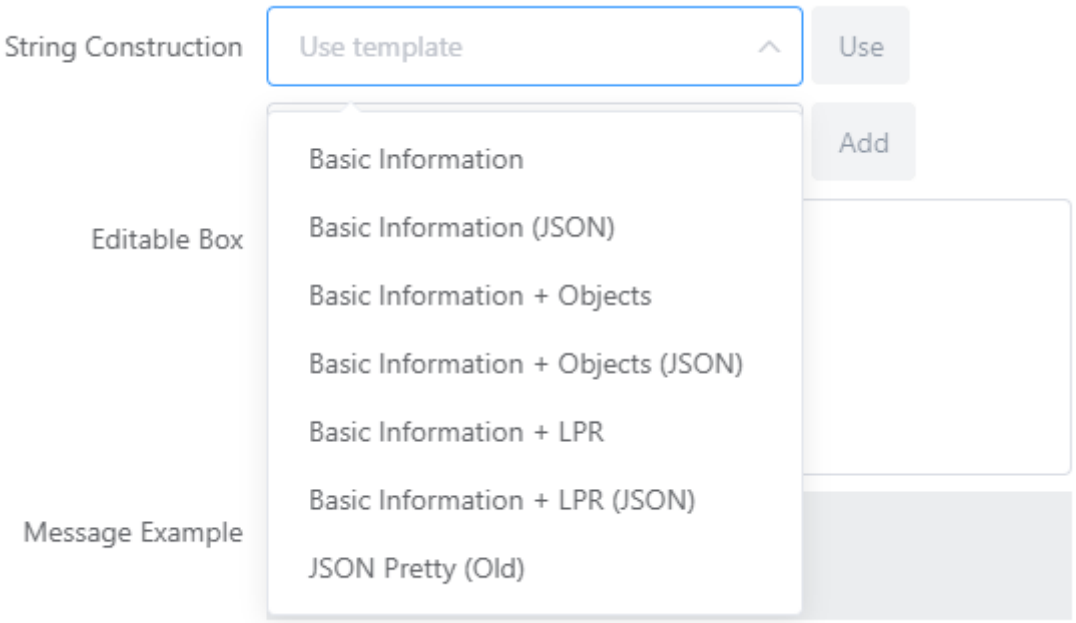
Edit box, Example box, and Test button

Typically, when composing a message, you type the message you want to send into the edit box. The typed message can contain an event metadata token in the form of {{XXX}} event metadata token. A list of available event metadata tokens is displayed in the Token Settings control dropdown list.

Click the Test button to actually send the hypothetical action message you see in the example box and test the integration with the recipient you're setting up.

Template Settings Controls

Use the Set Template control to set an action message in the form of a predefined template directly in the edit box.



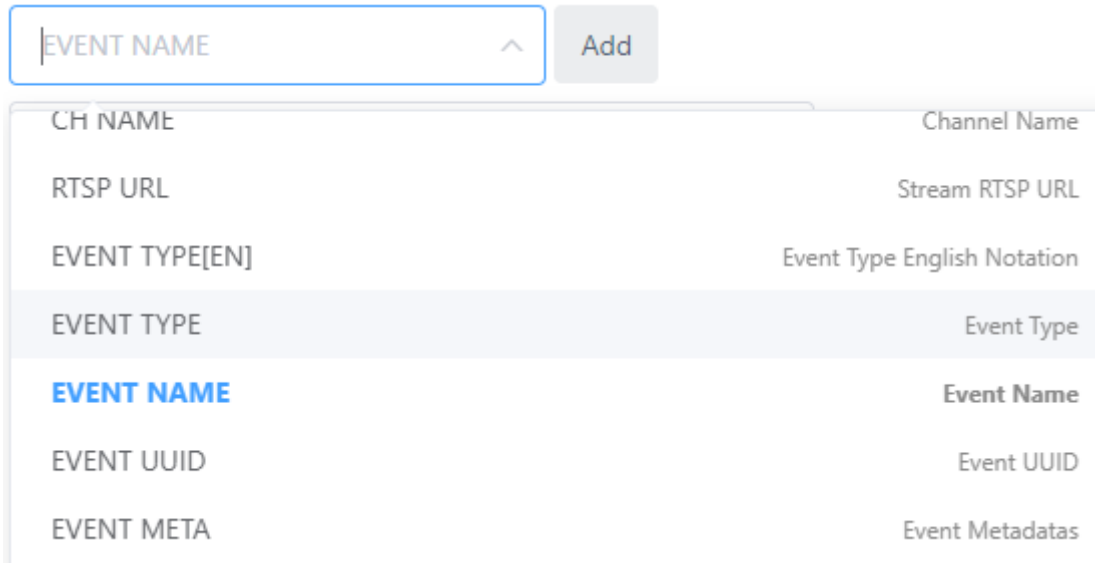
1. Select the template you want to set from the drop-down list.
2. Click the Use button on the right.

※Caution

When you use a template message, everything in the edit box is replaced with the template message. If you are working on something, you will lose your work if you replace it with the template message, so be careful when using it.

Token Settings Controls

You can insert event metadata into the action message using the Token Settings control.



1. Select the token you want to set from the drop-down list.

2. Click the Add button on the right.

The selected event metadata token is added to the edit box, and the virtual event metadata appears in the example box.

The token string can be moved anywhere in the edit box. The list of supported tokens and details of each are described below in the manual.

How to use logical condition token {{IF Statement}}

If you use a logical token among the event metadata tokens, you can output a statement only if the corresponding status-condition (Statement) is satisfied.

To use the logical condition token, {{IF Statement}} Context {{FI}} form should be used.

The {{IF Statement}} and {{FI}} are markers to indicate the beginning and end of the conditional statement, respectively.

Anything in between will only be shown if the condition is true. If the condition is not met, that portion will be ignored and skipped.

The Statement at the moment the event occurs determines whether Context is output.

You can use Arm/Disarm status and Event Type as conditions.

The rules for using logical tokens are as follows.

- {{IF XXX}} and {{FI}} must be paired.
- It can be used with other event metadata tokens. ex) {{IF XXX}} {{CH NAME}} {{FI}}
- It can also be used with object tokens.
- {{IF }} token cannot be nested. Cannot be used as in the following example. ex) {{IF AAA}} {{IF BBB}} {{FI}} {{FI}}

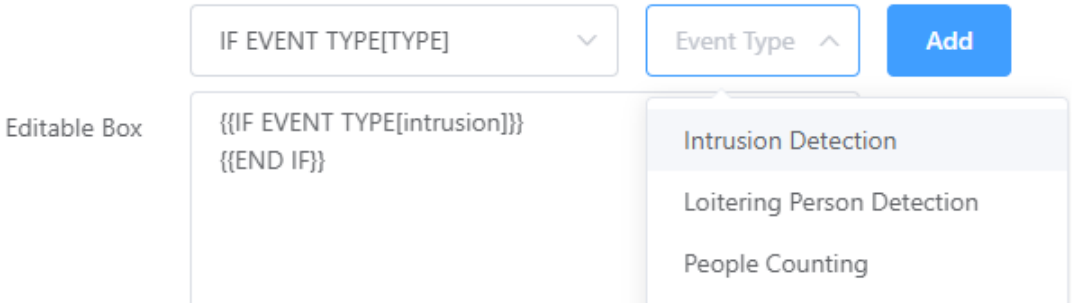
1st Example of using a condition token

Editable Box

```
{{IF DISARM STATUS[arm]}}
Arming
{{END IF}}
{{IF DISARM STATUS[disarm]}}
Disarming
{{END IF}}
```

When used as a message in the action of the Disarm system event, as in the example, it can output different sentences depending on the Arm/Disarm state.

2nd Example of using a condition token



When you add IF EVENT TYPE, you'll see a combo box where you can select the event type.

3rd Example of using a condition token

Editable Box

```
{
   "ch": "{{CH}}",
   "event_name": "{{EVENT NAME}}",
   "date": "{{TIME}}",
   "utc_timestamp": "{{TIMESTAMP}}",
   "mac": "{{MAC}}",
   "objects": [{{LIST OBJECTS[PARAM=COMMA]}}{
{{IF EVENT TYPE[intrusion]}}
         "track_id": {{::OBJ[TRACK ID]}},
{{END IF}}
         "class": "{{::OBJ[CLASS]}}",
         "bbox": {
            "x1": {{::OBJ[BBOX_X1]}},
            "y1": {{::OBJ[BBOX_Y1]}},
            "x2": {{::OBJ[BBOX_X2]}},
            "y2": {{::OBJ[BBOX_Y2]}}
         }
      } {{LIST OBJECTS[PARAM=COMMA]}}
   ]
}
```

This is an example of using IF tokens as part of the object token usage. The track_id is only shown if the Event Type is Intrusion.

4th Example of using a condition token

Editable Box

```
{{IF EVENT TYPE[loitering]}}
{{LIST OBJECTS}}
  "track_id":{{::OBJ[TRACK ID]}}
{{LIST OBJECTS}}
{{END IF}}
```

This is an example of using the entire object token as the content of the IF token. The Object List is only output if the Event Type is Loitering.

How to use object token {{::OBJ[XXX]}}

In the list of event metadata tokens, tokens of the form {{::OBJ[XXX]}} must be used according to specified rules. {{::OBJ[XXX]}} is a token representing different information about the object(s) causing the event.

An event may contain multiple objects, and the event's object information token is repeatedly replaced by object count.

Therefore, to specify where to repeat the syntax from and to for object information tokens, you must use a separate token, which is a list of objects.

The rules for using the OBJ token are as follows.

- All {{::OBJ[XXX]}} tokens must be placed between two {{LIST OBJECTS}} or {{LIST OBJECTS[PARAM=COMMA]}} tokens, with the first LIST token signifying the start of the iteration and the second LIST token signifying the end of the iteration.
- All {{::OBJ[XXX]}} tokens must be placed between two {{LIST OBJECTS}} or {{LIST OBJECTS[PARAM=COMMA]}} tokens, with the first LIST token signifying the start of the iteration and the second LIST token signifying the end of the iteration.
- A list of object information starting with {{LIST OBJECTS}} and ending with {{LIST OBJECTS[PARAM=COMMA]}} and a list of object information starting with {{LIST OBJECTS[PARAM=COMMA]}} must both end with {{LIST OBJECTS[PARAM=COMMA]}}.
- Object information enclosed in {{LIST OBJECTS}} has no delimiter to separate the items, and the string inside the list is simply repeated.
- {{LIST OBJECTS[PARAM=COMMA]}} appends a comma (",") character to separate items in the list.

To understand how to use the rule, see the following sample.

1st Example of using an object token

The "{{LIST OBJECTS}}" token repeats the string between it and the next "{{LIST OBJECTS}}" token for the number of event objects. The message between the {{LIST OBJECTS}} is repeated twice because the fictional event used to construct the example message contains two person objects.

In the above example, the string is “{{::OBJ[CLASS]}}” and “{{::OBJ[CLASS]}}[newline]”. This has resulted in a different message in the example field.

2nd Example of using an object token

Editable Box

```
{{LIST OBJECTS}}Class: {{::OBJ[CLASS]}}
Bounding Box: P1({{::OBJ[BBOX_X1]}}, {{::OBJ[BBOX_Y1]}}) P2({{::OBJ[BBOX_X2]}}, {{::OBJ[BBOX_Y2]}})

{{LIST OBJECTS}}
```

Message Example

```
Class: person
Bounding Box: P1(0.145877, 0.56192) P2(0.158819, 0.63)

Class: person
Bounding Box: P1(0.093212, 0.512331) P2(0.121459, 0.585929)
```

It is an example message sending object information by adding the bounding box positions of two persons’ objects containing a fictional event. The plain text remains the same, and the OBJ token repeats the object information syntax twice the number of objects.

3rd Example of using an object token

Editable Box

```
[{{LIST OBJECTS[PARAM=COMMA]}}{
   "event_name": "{{EVENT NAME}}"
   "class": "{{::OBJ[CLASS]}}",
   "bbox": [{{::OBJ[BBOX_X1]}}, {{::OBJ[BBOX_Y1]}}, {{::OBJ[BBOX_X2]}}, {{::OBJ[BBOX_Y2]}}],
}{{LIST OBJECTS[PARAM=COMMA]}}]
```

Message Example

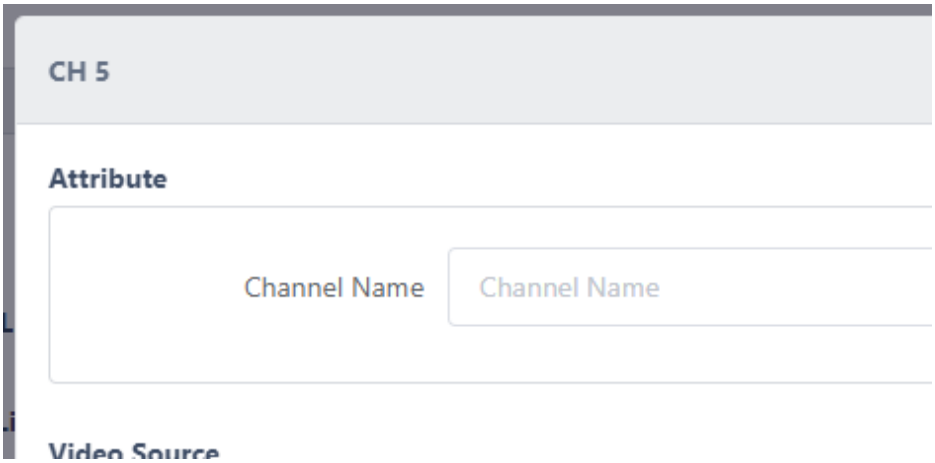
```
[{
   "event_name": "My Event Name"
   "class": "person",
   "bbox": [0.145877, 0.56192, 0.158819, 0.63],
},{
   "event_name": "My Event Name"
   "class": "person",
   "bbox": [0.093212, 0.512331, 0.121459, 0.585929],
}]
```

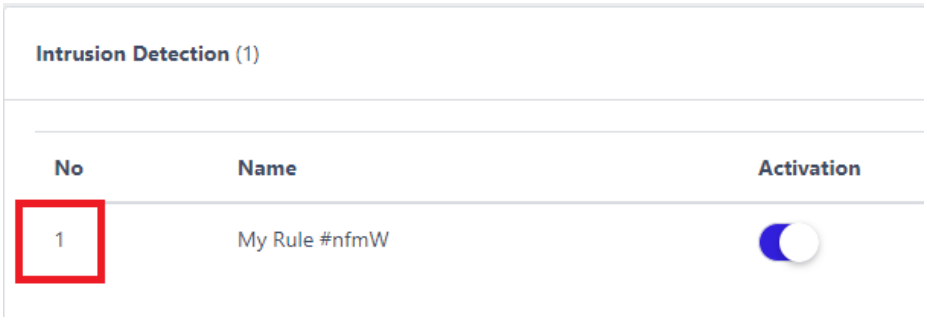
If you use the {{LIST OBJECTS[PARAM=COMMA]}} token to enclose the phrases of the list of object information, it will add a comma (,) between each phrase if there is more than one event object.

You can use this to build JSON strings, even if you use repeating object information sentences.

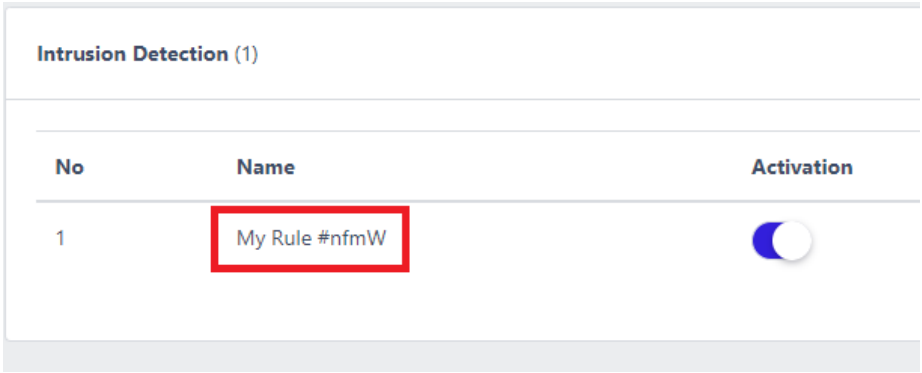
Event Metadata Token List

This section describes each of the supported event metadata tokens.
The event metadata tokens are categorized into four groups: event source, event information, object information, and time information about the object that generated the event.

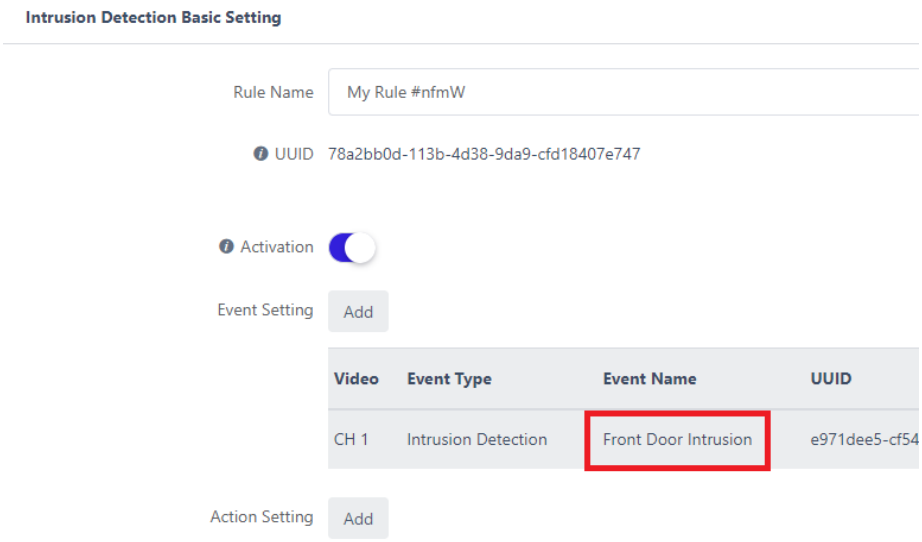
1. Event sources and information
   It is a list of tokens for basic information about the event, such as where it happened on what equipment.
   - {{CH}}
     - The channel number where the event occurred (1-8)
   - {{CH NAME}}
     - Channel name where the event occurred
     - Video Source – the channel name specified in the video stream setup
     - 

   - {{MAC}}
     - Device MAC address
   - {{DEVICE NAME}}
     - The name of the device as seen in the top left of the device's WebUI. Characters length includes the Mac address you set.
   - {{RULE NO}}
     - The action rule ID containing the event
     - 

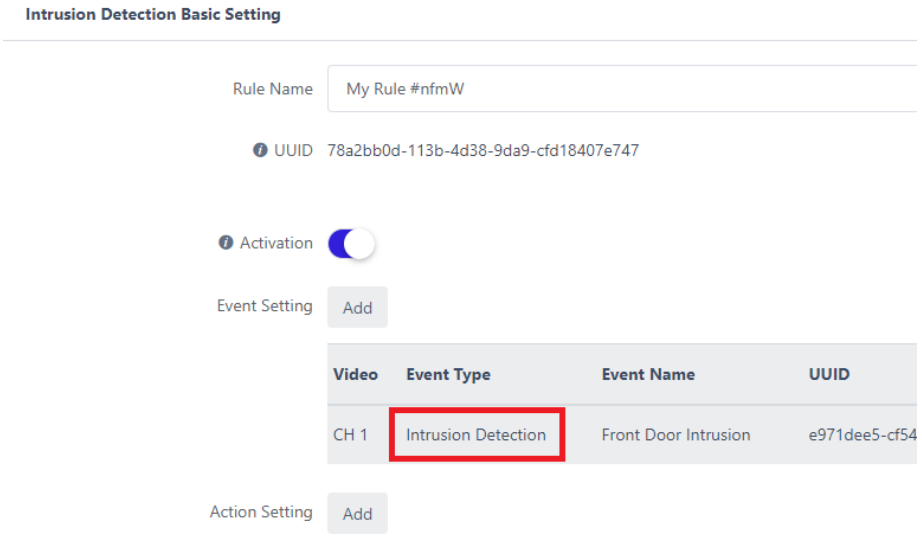
   - {{RULE NAME}}
     - The action rule name containing the event



- {{EVENT NAME}}
  - Event name



- {{EVENT TYPE}}
  - Event type



- {{EVENT TYPE[EN]}}

        - It will always have an English EVENT_TYPE value, and the value will not change based on the language set.
    - {{# OF OBJECTS}}
        - Number of event objects
    - {{COMBINED COUNT}}
        - In events in counting apps such as Occupancy, PeopleCounting, VehicleCounting, and Advanced Visitor Analytics, the summed count value of the event target counter at the time of the event.

2. Event time-related tokens
   For example, if the event was at 18:43:9.739 on 7 March 2023 in the GMT+9:00 time zone, each time token would be replaced as follows.
    - {{TIME YYYY-MM-DD}}
        - Event date ex) 2023-03-07
    - {{TIME YYYYMMDD}}
        - Event date ex) 20230307
    - {{TIME DD/MM/YYYY}}
        - Event date ex) 07/03/2023
    - {{TIME YYYY}}
        - Event year with 4-digit ex) 2023
    - {{TIME YY}}
        - Event year with 2-digit ex) 23
    - {{TIME mm}}
        - Event month with 2-digit ex) 03
    - {{TIME dd}}
        - Event date with 2-digit ex) 07
    - {{TIME HH}}
        - Event occurrence hour on a 24-hour basis ex) 18
    - {{TIME MM}}
        - Event occurrence minute with 2-digit ex) 43
    - {{TIME SS}}
        - Event occurrence second with 2-digit ex) 09
    - {{TIME MS}}
        - Event occurrence millisecond ex) 739
    - {{TIMESTAMP}}
        - Timestamp of the event occurrence time ex) 1678182189.739000
    - {{TIME ISO8601}}
        - ISO8601 standard format for the event occurrence time ex) 2023-03-07T18:43:09.739000+09:00
    - {{UTC ISO8601}}

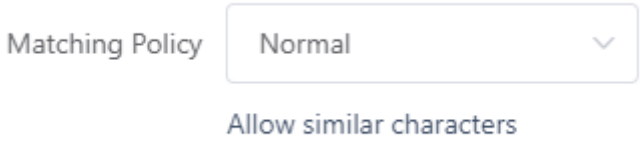
        - UTC time in ISO 8601 standard format for the event occurrence time ex) 2023-03-07T09:43.09.739000+00:00
    - {{TIME}}
        - Event time format as designated ex) 07 March 2023 18:43:09

3. logical condition token
    - {{IF DISARM EVENT[arm]}}
        - The beginning of an IF logical condition token. Only when Disarm is arm in the Disarm event as a condition, it shows the sentence between {{IF}} and {{FI}}
    - {{IF DISARM EVENT[disarm]}}
        - The beginning of an IF logical condition token. Only when Disarm is disarm in the Disarm event as a condition, it shows the sentence between {{IF}} and {{FI}}
    - {{IF EVENT TYPE[TYPE]}}
        - The beginning of an IF logical condition token. Only when the Event Type matches a character in the TYPE position as a condition, it shows the sentence between {{IF}} and {{FI}} ex) {{IF EVENT TYPE[loitering]}}
    - {{FI}}
        - The end of an IF logical condition token. An IF token must be paired with an FI token.

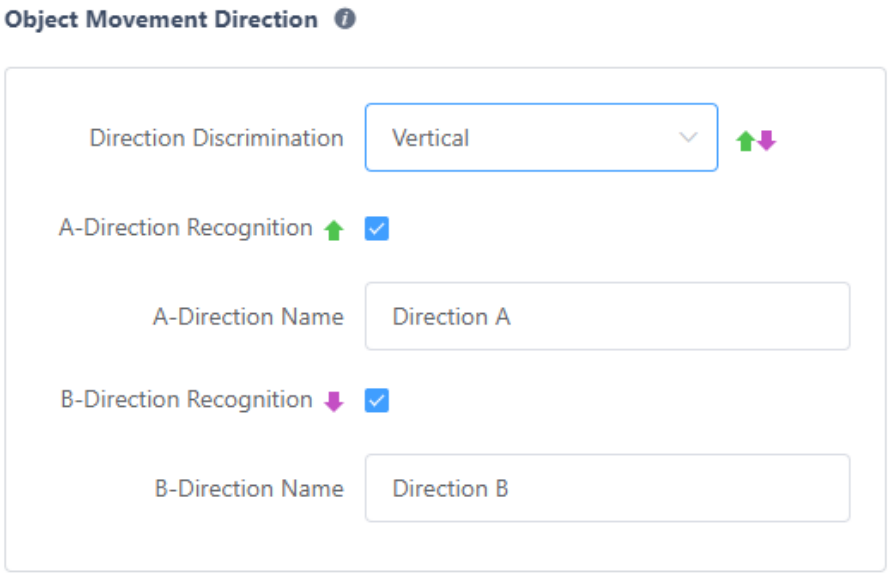
4. Token for object information
    - {{LIST OBJECTS}} ~ {{LIST OBJECTS}}
        - Repeat as many times as objects to output the internal syntax.
    - {{LIST OBJECTS[PARAM=COMMA]}} ~ {{LIST OBJECTS[PARAM=COMMA]}}
        - Use commas (,) to separate repeated statements, and repeat the internal syntax as many times as there are objects
    - {{::OBJ[INDEX]}}
        - The event object's index, starting from 0
    - {{::OBJ[TRACK ID]}}
        - Object tracking ID
    - {{::OBJ[CLASS]}}
        - Object class. Different apps and event types detect different objects.
        - person / car / bike / violence / fire / abandoned / animal / man / woman / helmet / no-helmet / vest / no-vest / fallen / lp / …
    - {{::OBJ[SCORE]}}
        - Object confidence score value
        - The value is for reference and is not appropriate to make a general judgment.
    - {{::OBJ[BBOX_X1]}}
        - The X coordinate of the top left point of the object's bounding box.
        - The coordinate system is normalized to 0-1. The left end is 0, the right end is 1.
    - {{::OBJ[BBOX_Y1]}}
        - The Y coordinate of the top left point of the object's bounding box

        - The coordinate system is normalized to 0-1. The top end is 0, the bottom end is 1.
    - {{::OBJ[BBOX_X2}}
        - The X coordinate of the right bottom point of the object's bounding box.
    - {{::OBJ[BBOX_Y2}}
        - The Y coordinate of the right bottom point of the object's bounding box.

5. Token for displaying LPR object information
   When using LPR object information, you must use {{LIST OBJECTS}} or {{LIST OBJECTS[PARAM=COMMA]}} to enclose the object display syntax, as with normal object information.
    - {{::OBJ[LP_TEXT_DETECTED}}
        - The plate number by License plate recognition
    - {{::OBJ[LP_TEXT_DB}}
        - The plate number registered to DB by the user
        - LP_TEXT_DETECTED and LP_TEXT_DB are usually the same. However, if you are using a loose matching policy, they may be matched even if they are not exact

          matches.
    - {{::OBJ[LP_GROUP_NAME]}}
        - Group name containing the user's registered plate number in DB.
        - If the number is in several groups at the same time, it is replaced by a comma (,) separated list of group names.
            - ex) Group 1, Group 2
    - {{::OBJ[LP_ID]}}
        - Index number registered in DB
    - {{::OBJ[LP_NOTE]}}
        - The note on the plate number the user has registered in DB.
    - {{::OBJ[LP_COUNTRY_CODE]}}
        - Country code of the recognized vehicle number
            - 2-digit alphabetic country code for LPR-EU. Replaced by EU if not detected.
            - 2-digit alphabetic state code for LPR-US. Replaced by US if not detected.
            - Replaced by JP for LPR-JP.
            - Replaced by KR for LPR-KR.
    - {{::OBJ[MOVEMENT_DIR]}}
        - The direction of movement of the recognized vehicle number (indicated by A or B).
    - {{::OBJ[MOVEMENT_DIR_NAME]}}
        - The event name you set for the direction of movement of the recognized vehicle number.



6. Object attributes information token
   When you activate the Basic Attributes app or the Advanced Attributes app, additional analysis of detected person's attribute information is performed.
   If you want to include object attribute information in an action message, the object display syntax should be start and end with {{LIST OBJECTS}} or {{LIST OBJECTS[PARAM=COMMA]}}.
   Please refer to the token information for representing the attributes below.
   - {{::OBJ[ATTR_TOP_COLOR]}}
     - Top clothes color
     - When top clothes color is analyzed, it will be replaced with one of red, orange, yellow, green, blue, purple, pink, brown, white, gray, black.
     - If the estimated top clothes color is unclear, it is replaced with an empty string.
   - {{::OBJ[ATTR_BOTTOM_COLOR]}}
     - Bottom clothes color
     - When bottom clothes color is analyzed, it will be replaced with one of red, orange, yellow, green, blue, purple, pink, brown, white, gray, black.
     - If the estimated bottom clothes color is unclear, it is replaced with an empty string.
   - {{::OBJ[ATTR_TOP_TYPE]}}
     - Top clothes type
     - When top clothes type is analyzed, it will be replaced with one of long_sleeve, short_sleeve, sleeveless, onepiece.
     - In the case of onepiece, it includes all types of clothing that are a single set of top and bottom, such as long padding.
     - If the estimated top clothes type is unclear, it is replaced with an empty string.
   - {{::OBJ[ATTR_BOTTM_TYPE]}}
     - Bottom clothes type
     - When bottom clothes type is analyzed, it will be replaced with one of long_pants, short_pants, skirt, none.
     - If the top clothes type is onepiece, bottoms can be none

        - If the estimated bottom clothes type is unclear, it is replaced with an empty string.
    - {{::OBJ[ATTR_GENDER]}}
        - Gender
        - When gender is analyzed, it will be replaced with one of man, woman.
        - If the estimated gender is unclear, it is replaced with an empty string.
    - {{::OBJ[ATTR_AGE]}}
        - Age group
        - If age group is analyzed, it will be replaced with one of child, teenager, adult, senior.
        - If the estimated age group is unclear, it is replaced with an empty string.
    - {{::OBJ[ATTR_ACCESSORIES]}}
        - Accessories
        - When accessories are analyzed, the token will be replaced with one of carrier, umbrella, bag, hat, glasses, none.
        - If the estimated gender is unclear, it is replaced with an empty string.
    - {{::OBJ[ATTR_PET]}}
        - Pet
        - If the presence or absence of a companion animal is analyzed, it is replaced with either yes or no.
        - If the estimated presence of the pet is unclear, it is replaced with an empty string.

Event-specific metadata

No metadata is provided for events not specified in the table.

event_type	**event(en)**	**meta1**	**meta2**	**meta3**
enter_exit	Enter/Exit Detection	Total count	Enter count	Exit count
fence	Virtual Fence	Total count	A direction count	B direction count
lpr_eu	LPR-Europe	Vehicle license plate	Vehicle group	Vehicle movement direction
lpr_jp	LPR-JP	Vehicle license plate	Vehicle group	Vehicle movement direction
lpr_kr	LPR-KR	Vehicle license plate	Vehicle group	Vehicle movement direction
lpr_us	LPR-US	Vehicle license plate	Vehicle group	Vehicle movement direction
multi_zone_occupancy	Multi Zone Counting	Count of objects in the zone	None	None
occupancy	Occupancy Counting	count	None	None
occupancy_car	Occupanc Car Counting	count	None	None

people_counting	People Counting	count	None	None
staff_exclusion	Staff Exclusion People Counting	count	None	None
vehicle_counting	Vehicle Counting	count	None	None
vehicle_presence	Vehicle Zone Presence	Status label	Occupied/Empty status label	occupied/free
visit_advanced	Advanced Visitor Analysis	count	None	None
vt_counting	Vehicle Type Counting	count	None	None
work_vehicle	Work Vehicle Hazard Detection	Status label	Danger/Safe status label	None
zone_occupancy	Zone Counting	Objects in the zone	None	None
alarmin	Alarm In	Alarm In name	Alarm In number	None
virtual_alarmin	Vitual Alarm In	Virtual Alarm In name	Virtual Alarm In number	None
disarm	Disarm	Change status	target(system, master, channels)	channel
login	Login	Change status	username	IP address
network	Network Error	DNS Recovery/Error	None	None
video	Video Loss/Recovery	Change status	channel	None

Event type key

Available from firmware version 104317.

AI APP:

key	event_type
abandon	Illegal Dumping
abandon_hyb	Illegal Dumping+
adv_heatmap	Advanced Heatmap
advanced_attr	Advanced Attribute
animal	Animal Detection
animal_hyb	Animal Detection+
animal_bear	Bear Detection
basic_attr	Basic Attribute
basic_heatmap	Heatmap
body_gaze	Intentional Body Gaze Detector
bullying	Bullying Detection
bullying_hyb	Bullying Detection+
calib_3d	Object Location Tracking
closecam_coveredface	CloseCam Covered Face
covered_face	Covered Face Detection
crowd	Crowd Detection
dpc	Dust-Proof Clothing Detection
enter_exit	Enter/Exit Detection
facemask	Dynamic Face Masking
fallen	Fallen Person Detection
fallen_hyb	Fallen Person Detection+
fence	Virtual Fence

fire	Fire & Smoke Detection
fire_hyb	Fire & Smoke Detection+
gun	Gun Detection
fld	Forklift Detection
forklift_ndd	Forklift Non-Driver Detection
forklift_nohelmet	Forklift No Helmet
hand_intrusion	Hand & Foot Intrusion
intrusion	Intrusion Detection
loitering	Loitering Detection
lpmask	LP Masking
lpr_an	LPR-일반
lpr_eu	LPR-Europe
lpr_jp	LPR-JP
lpr_kr	LPR-KR
lpr_us	LPR-US
multi_zone_occupancy	Multi Zone Counting
no_helmet	Helmet Not Wearing
no_mask	No Mask
no_ppe	No PPE
occupancy	Occupancy Counting
occupancy_car	Occupancy Car Counting
outofuniform_hyb	Out of Uniform
people_counting	People Counting
phone_walk	Phone Walk Detection
pmask	Dynamic Privacy Masking
prolonged_stay	Human Prolonged Stay
ptz_tracking	PTZ Tracking
queue	Queue Management
queuelimit_hyb	Queue Limit
reverse_movement	Reverse Movement Detection
road_pedesrian	Road Pedestrian Detection
speed_anomaly	Speed Anomaly Detection
spill	Spill Detection
staff_exclusion	Staff Exclusion People Counting
stay_go	Stay & Go
stopping	Stopping Detection
tailgating	Tailgating
thermal	Thermal Intrusion Detection
threat	Imminent Threat
threat_hyb	Imminent Threat+
underage	Age Filter
unsafe_lifting	Unsafe Lifting
vehicle_counting	Vehicle Counting
vehicle_presence	Vehicle Zone Presence
violence	Aggressive Detection
violence_hyb	Aggressive Detection+
visit_advanced	Advanced Visitor Analysis
vqm	Vehicle Queue Management
vt_counting	Vehicle Type Counting
vtd	Vehicle Type Detection
work_vehicle	Work Vehicle Hazard Detection
zone_occupancy	Zone Counting

SYSTEM EVENT

key	event_type
alarmin	Alarm In
virtual_alarmin	Virtual Alarm In
generic	Generic Event
video_loss	Video Loss
video_recovery	Video Recovery
storage	Storage Device Error
boot	System Start
factory	Factory Default
disarm	Disarm
heartbeat	Recurrence
login	Login
tamper	Tamper Detection
network	Network Error
Deprecated	
video	Video Loss / Recovery

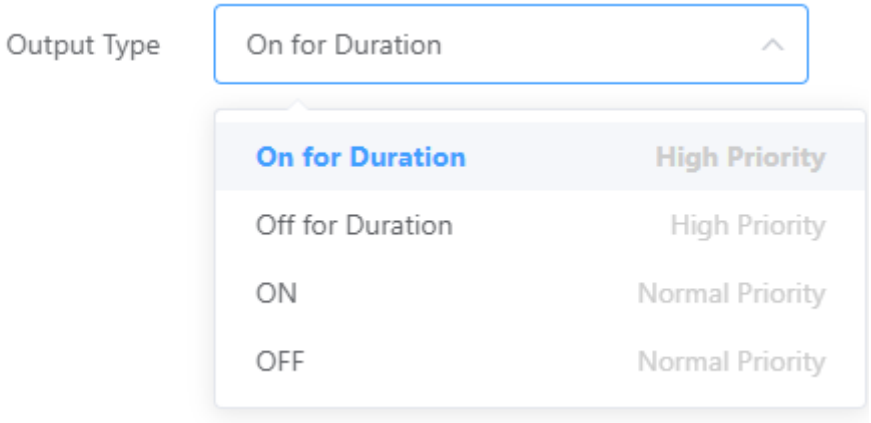
System Action Handler

Relay

Relays are functions that output digital signals through device I/O terminals. Relays can be used to control a warning light or to operate with a door lock as a door control signal.

Relay actions can be added from the Action Settings.

Select the action type to **Relay**, you'll see the relevant settings at the bottom.



The relay's output type is actually two settings, ON/OFF, but the settings screen is configured to allow you to select four different items. The definitions for each output type are as follows.

Output type	Description	Priority
On for Duration	ON output maintains during the duration time	High
Off for Duration	ON output maintains during the duration time	High
ON	Changes alarm output status to ON	Normal
OFF	Changes alarm output status to OFF	Normal

You'll notice that the right side of each output type describes its priority. Since there are a limited number of relays, and many event action items can be assigned to them, this creates an issue of control over the relay device.

※ Relay type control policy

1. If multiple relay actions are the same priority, the last one to occur takes control

2. If a higher and lower priority actions are competing, the higher relay type takes control. Higher priority alarms have a duration, so the last lower priority action takes control after the time elapses.

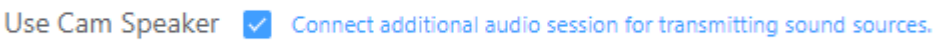
3. Low-priority items have no duration, so they permanently change the default state of the output until a new request is made by another event action.

Camera speaker Output

If IP camera connected to the AIBOX supports audio output through speakers, you can drive an event action to emit audio output.
Camera speaker output operates based on the protocols defined by the ONVIF Audio Backchannel standard.

※ Preconditions

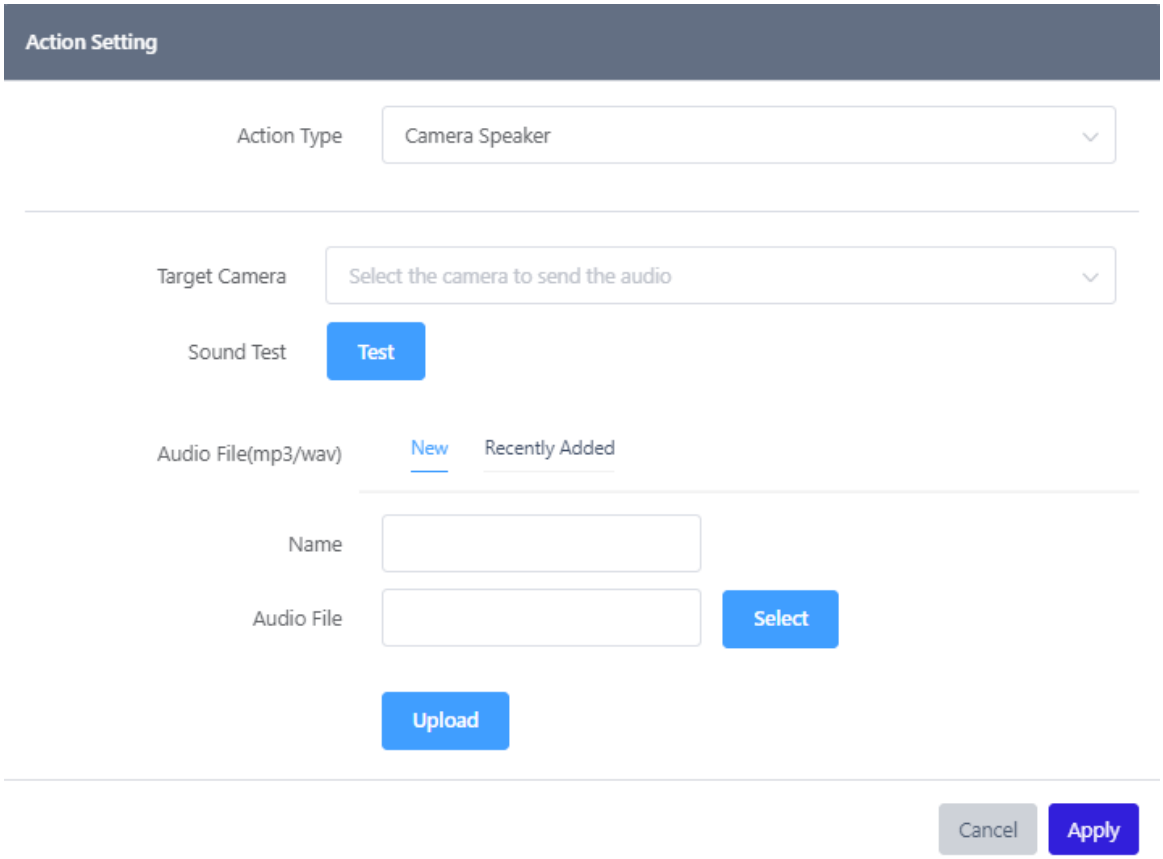
To run the Camera Speaker Output action, you must set the video stream to connect an additional audio session for sound transmission.
Make sure the following settings are checked for the camera you want to use in the **Video stream – Etc** settings.



Action Settings

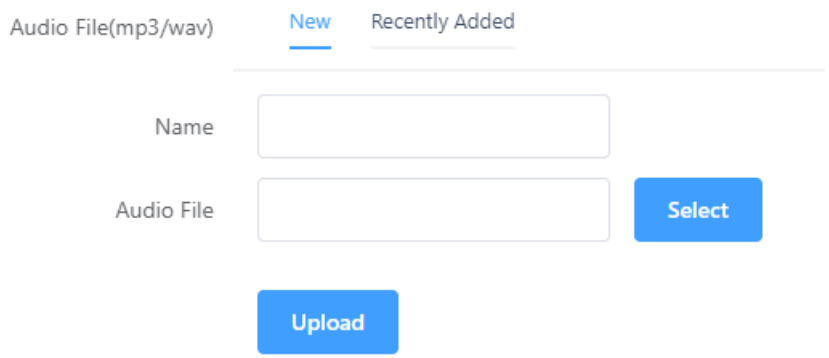
The camera speaker output action can be added from the Action Settings.

1. Select the Action Type to **Camera Speaker**, then, the relevant settings at the bottom.

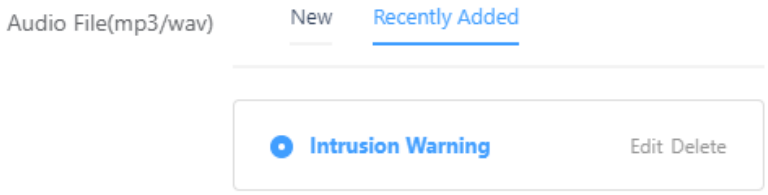


2. Select a camera connected to the AIBOX to output speaker sound

3. Select a sound source to send to the camera. Sound files can be uploaded on the **New** menu. MP3 and WAV formats are available.



Alternatively, select the audio file on the existing list to send to the camera.

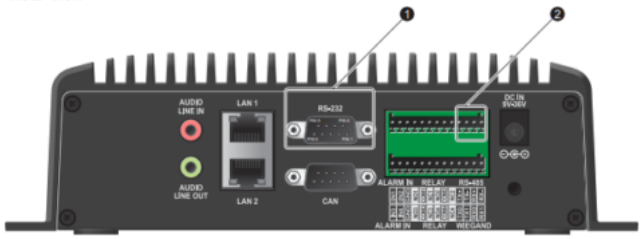


RS485 (RS232)

You can send messages through the RS485 or RS232 interface when an application event occurs. (RS232 is not supported on some models.)

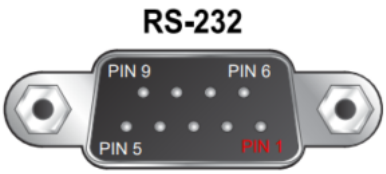
Basic Interface Wiring

- Rear View



❶ RS-232 (DB-9) Connector Pinout

Below is the pinout of a typical 9 pin RS-232 connector, this connector type is also referred to as a DB-9 connector.
A computer's COM port (DTE) is usually male, and any peripheral devices you connect to this port usually have a female connector (DCE).



Pin	Signal	DTE Signal Direction	Description
1	-	-	-
2	RXD	IN	Receive Data : Pin 2 (RXD) is connected to Pin 3 (TXD) of another device.
3	TXD	OUT	Transmit Data : Pin 3 (TXD) is connected to Pin 2 (RXD) of another device.
4	-	-	-
5	GND	-	Signal Ground : Pin 5 (GND) is commonly connected across all devices.
6	-	-	-
7	-	-	-
8	-	-	-
9	-	I-	-

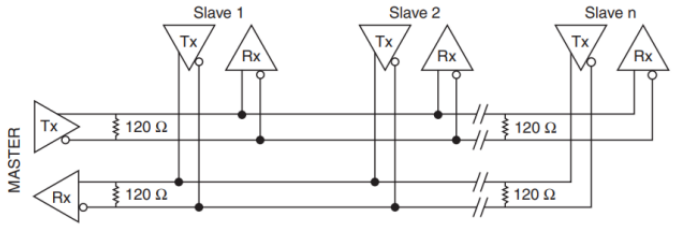
❷ RS-485 Connector Pinout

Pin	Signal	Signal Direction	Description
1	TX+	Transmit Data+	Device A's TX+ is connected to Device B's RX+
2	TX-	Transmit Data-	Device A's TX- is connected to Device B's RX-
3	RX+	Receive Data+	Device A's RX+ is connected to Device B's TX+
4	RX-	Receive Data-	Device A's RX- is connected to Device B's TX-

RS-485 Topologies

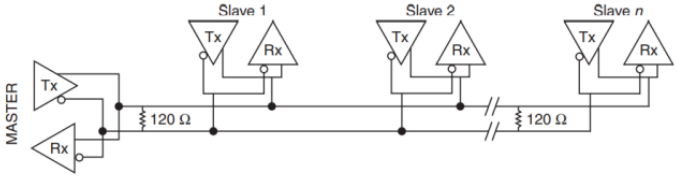
Connecting RS485 4-wire to 4-wire (Full Duplex)

This is an example of a standard 4-wire RS485 device to RS485 device configuration.



Connecting RS485 4-wire to 2-wire (Half Duplex)

For 2-wire transmission, you will need to short the transmit (TXD) and receive (RXD) signals together on the RS-485 port.
Wire the 2-wire device's send pin (TXD) to both TXD- and RXD-. Wire the device's receive pin (RXD) to both TXD+ and RXD+.



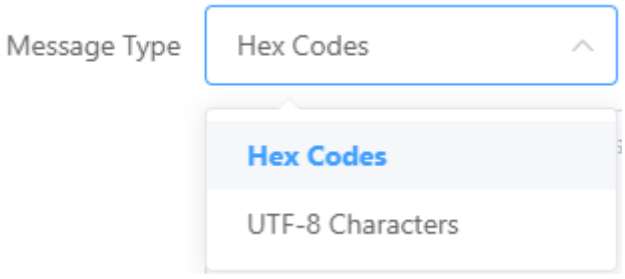
Action Setup

The setup procedures for RS485 and RS232 are the same, with the only difference being the output interface.

You can add an RS485 or RS232 action from the action settings screen.

When you set the **Action Type** to **RS485**, the related settings will be displayed below.

Message Type

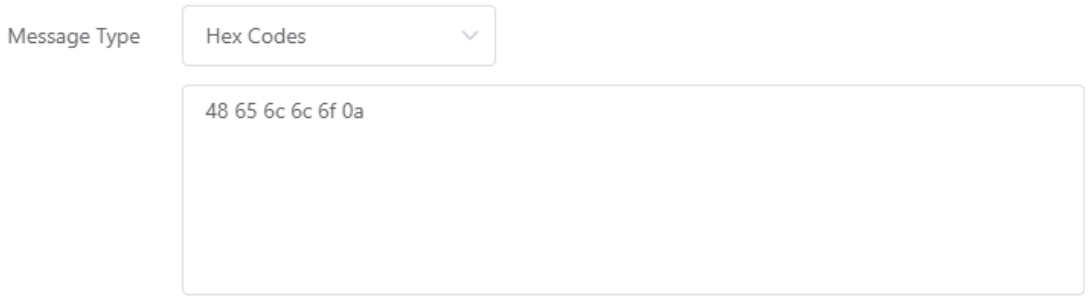


You can set the message type to either Hex Codes or UTF-8 formats. The default setting is Hex Codes.

Hex Codes

When you select the Hex Codes format, you can transmit binary data using hexadecimal values. Event metadata tokens cannot be used when transmitting binary data; instead, you must use fixed binary data. Please refer to the setup example provided.

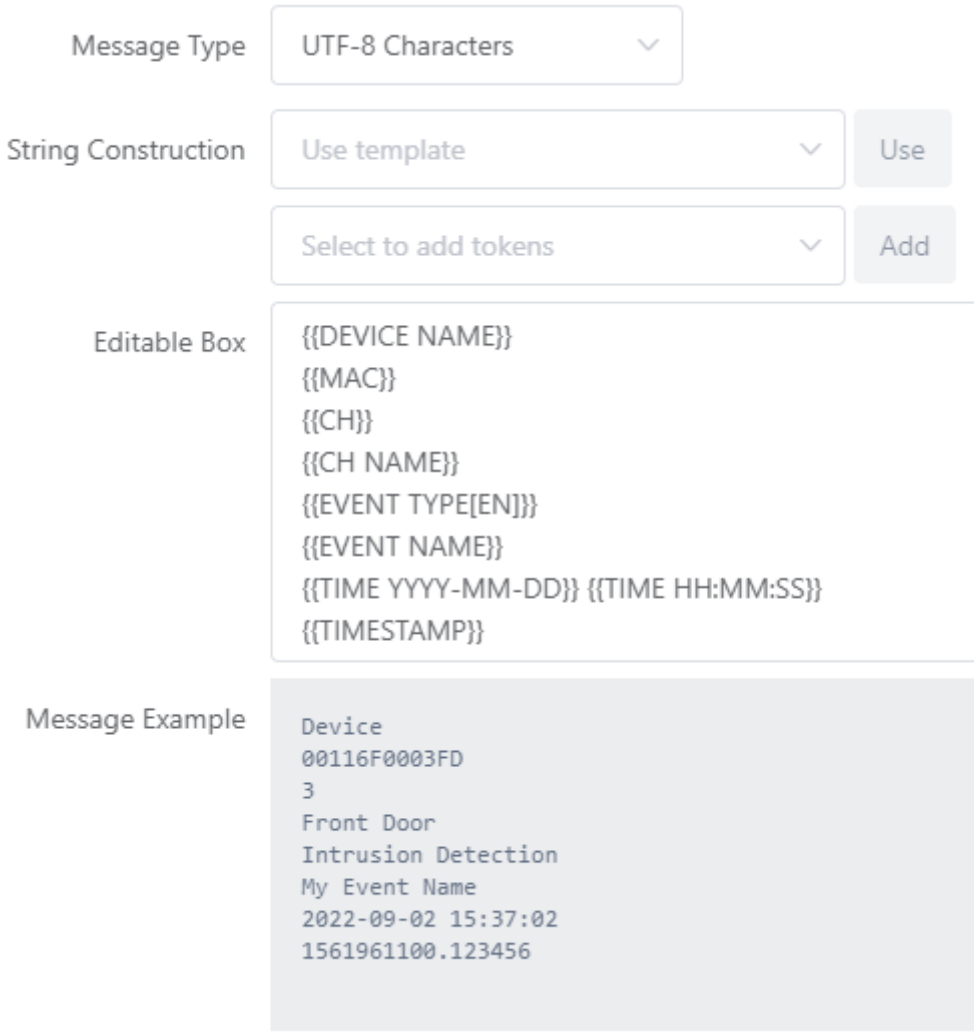
Setup Example



UTF-8

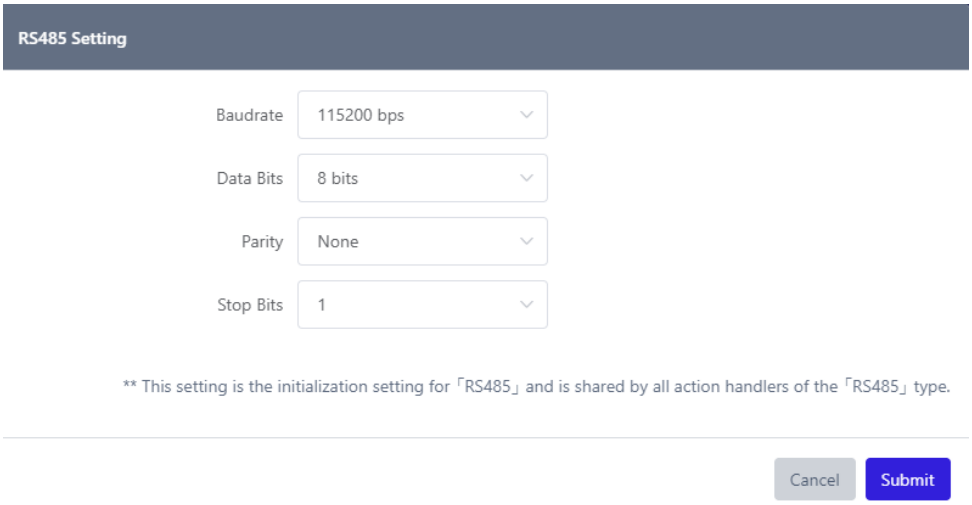
The UTF-8 format allows settings to be configured using Tokens and templates. Please refer to the setup example provided.

Setup Example



RS485 (RS232) Setting

Configure Baudrate, DataBits, Parity, and StopBits. These settings are shared across all items of the same action type. Therefore, if you change settings in a specific action handler, it will apply to all action handlers.



RS485 Modbus (Satel)

1. Introduction

1.1 Prerequisites

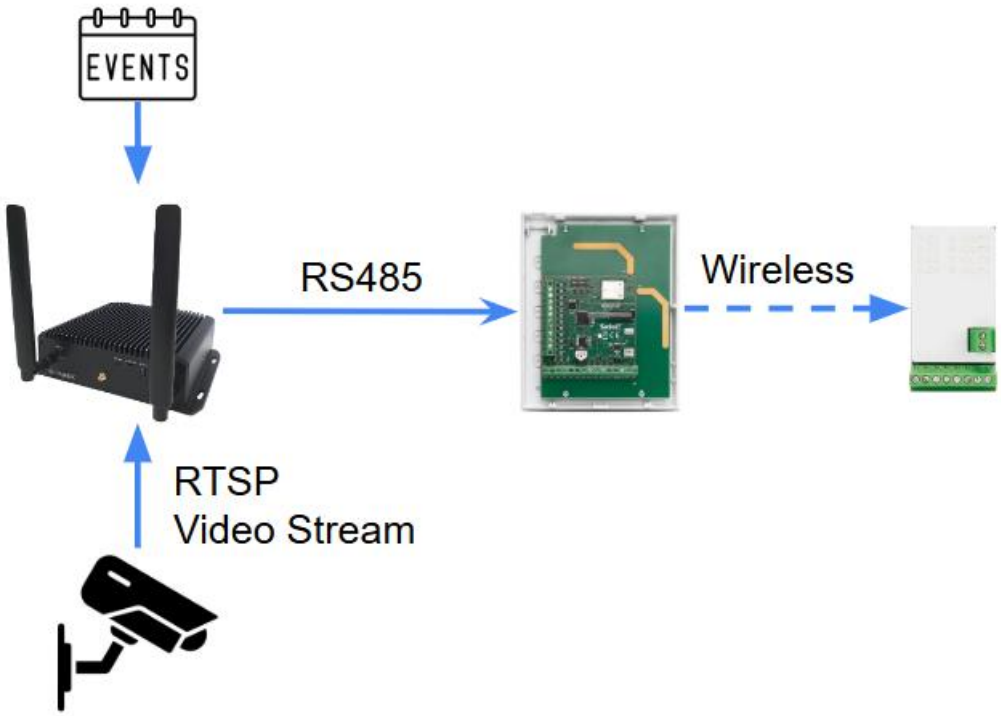
- AIBOX FW version 103813 or higher.
- RS485 Modbus Relay Box

Recommended Alarm Box models:

- ACU-220

1.2 Learn about integration architecture

When an event occurs, the AIBOX transmits a signal to the ACU-220 via RS485, combined with video. The ACU-220, as a wireless system controller, transmits the signal to control the devices connected wirelessly. The advantage of this usage is that up to 48 relays can be controlled through the ACU-220, and since it uses wireless communication, there is no need for additional cables such as LAN cables.



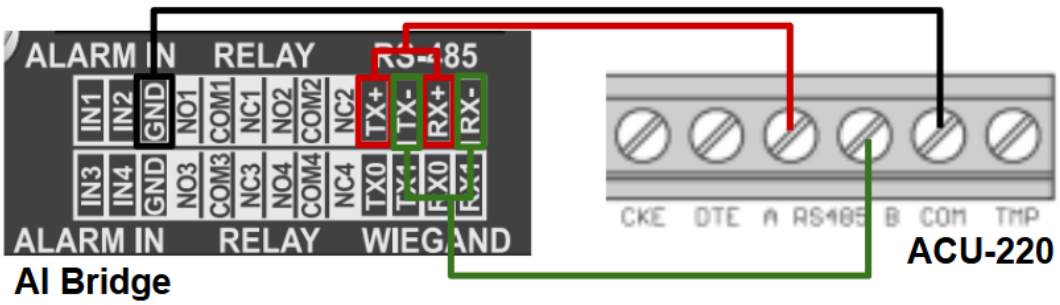
2. Configuration

2.1 HW wiring method

2.1.1 Wiring method for connecting the ACU-220 and AIBOX

The AIBOX uses full-duplex communication, while the AI BOX uses half-duplex communication, so the connection method differs due to hardware differences. Please follow the steps below.

Connect the RS485(RX+) and RS485(TX+) of the AIBOX, and connect the RS485(RX-) and RS485(TX-) as well. We will refer to these as RS485(D+) and RS485(D-) going forward. Connect either RX or TX from the RS485(A) of the ACU-220 to the RS485(D+) of the AIBOX. Similarly, connect either RX or TX from the RS485(B) of the ACU-220 to the RS485(D-) of the AIBOX. Finally, connect the COM of the ACU-220 to the GND of the AIBOX.



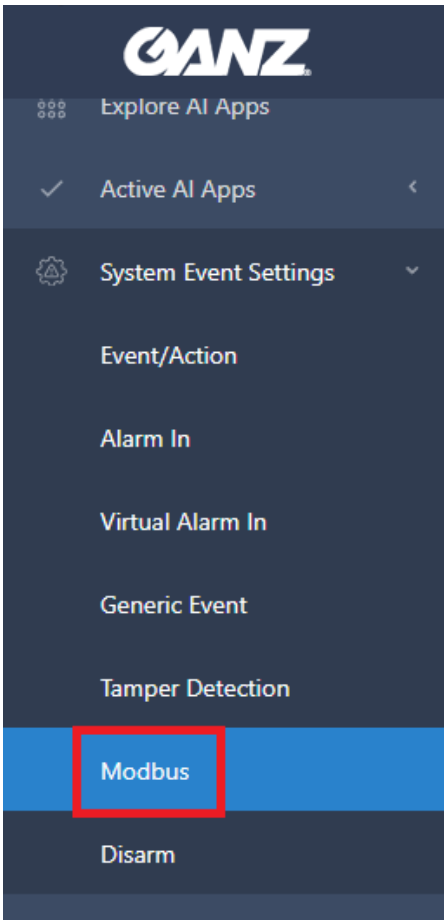
2.2 AIBOX

Here are the steps to configure the AIBOX for use with Modbus equipment.

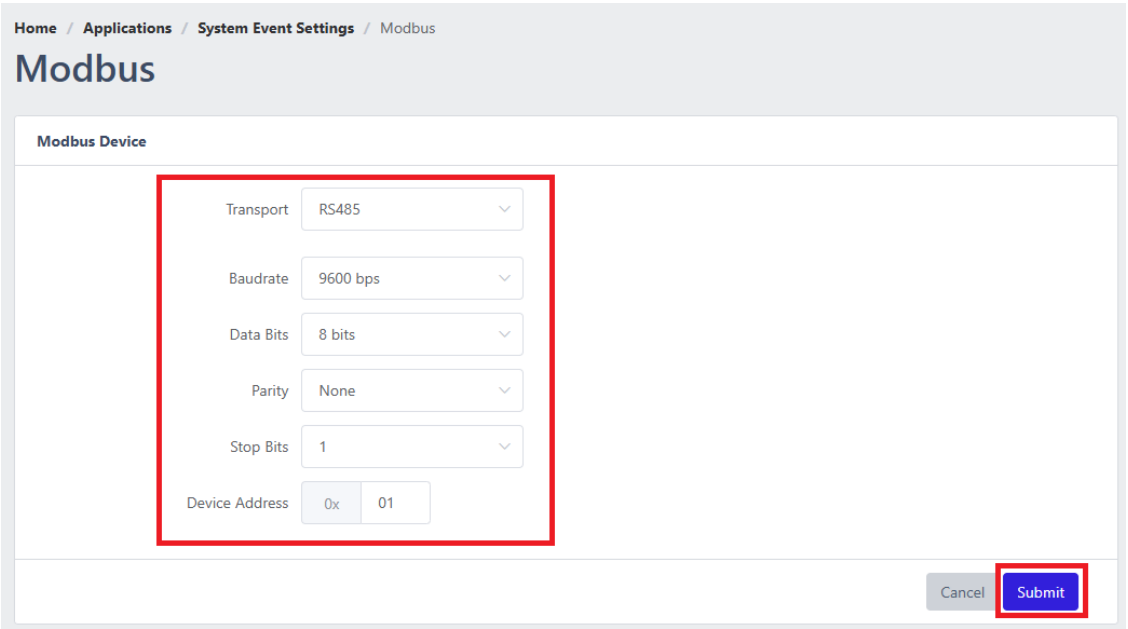
Before configuring the AIBOX, you must complete the setup of the ACU-220 device. Please refer to the Satel manual or FAQ.

2.2.1 Modbus Relay Setting

Log in to the AIBOX, then click “Modbus” under “System Event Settings” in the “APP SETTINGS” menu on the left sidebar.



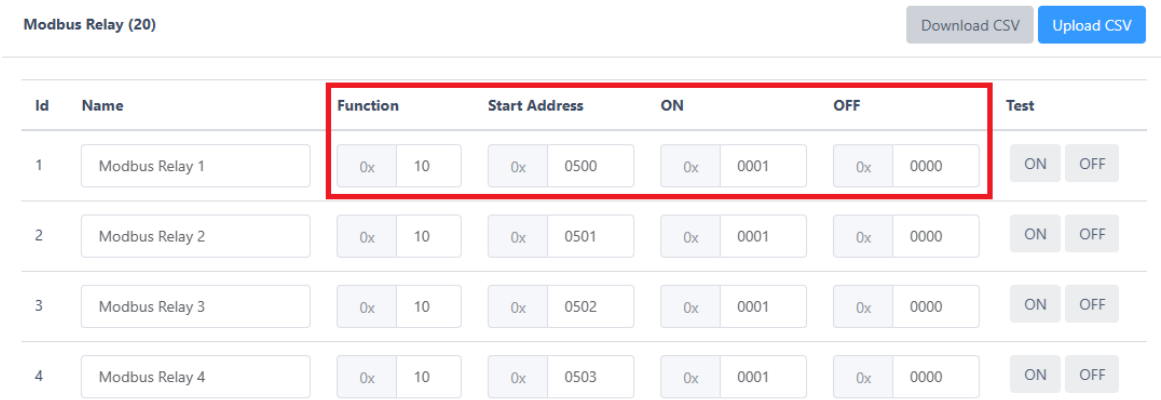
Select RS485 for Transport, then choose the Baudrate, Data Bits, Parity, and Stop Bits to use, and enter the Device Address.



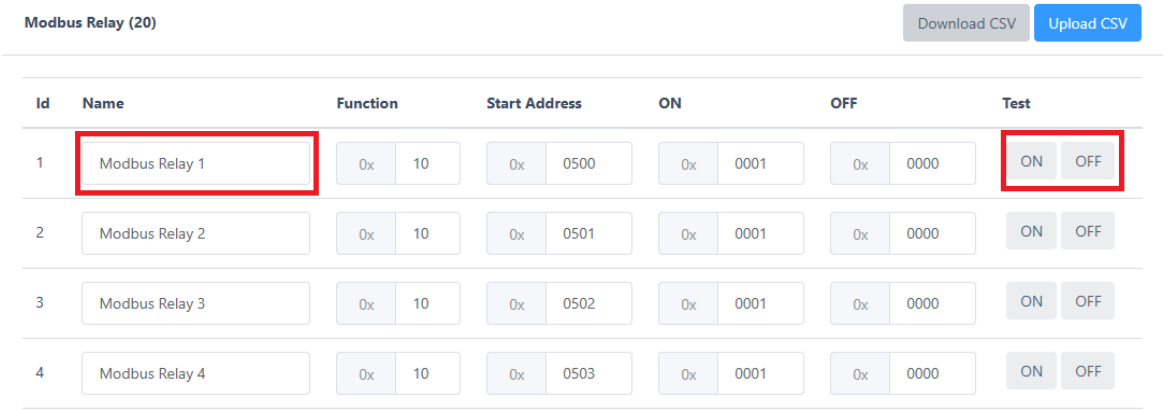
Note. Each configuration value must match the MODBUS settings configured on the ACU-220.

Tip. The Baudrate of the ACU-220 supports a range from 1200 to 19200 bps.

Enter the following configuration values: For the ACU-220, the Function is fixed at 0x10, the Start Address increases by 1 starting from 0x0500, ON is 0x0001, and OFF is 0x0000.



Tip. You can set the name of the Relay you wish to use and click the ON/OFF button to test it.

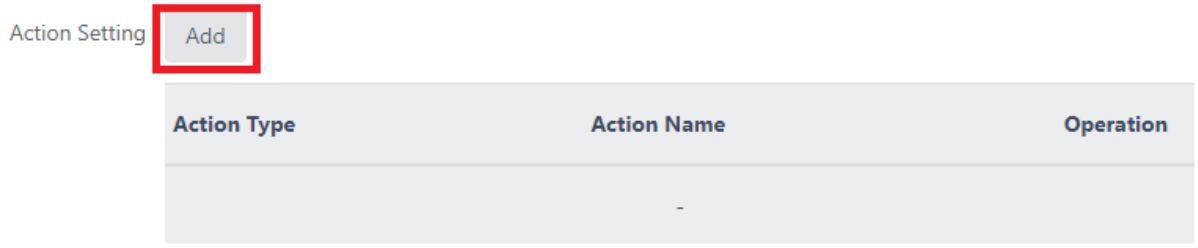


Note. If the command is successfully received by the ACU-220, the red LED in the center of the device will turn off or on. (If it was off initially, it would turn on; if it was on, it would turn off.)

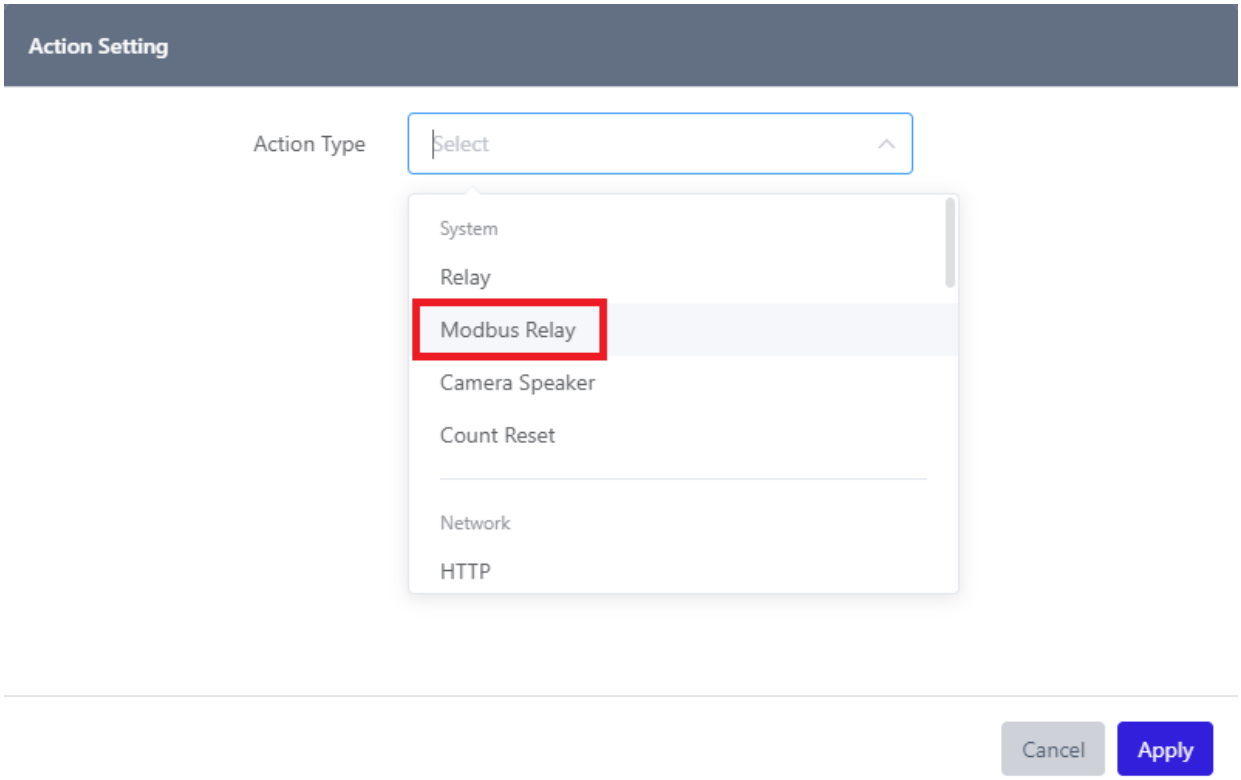
2.2.2 Modbus Relay action

Below are the instructions for adding the Relay device registered in the AIBOX to the action settings.

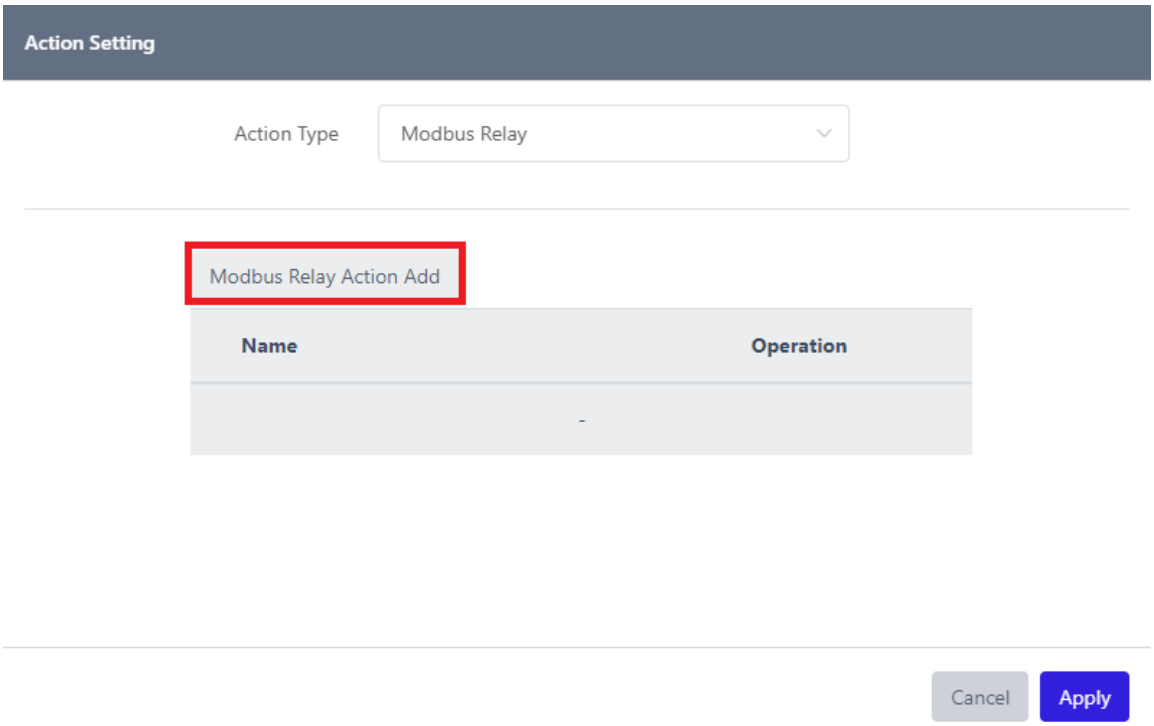
After setting up the AI App or system events, click on Action setting and then select Add.



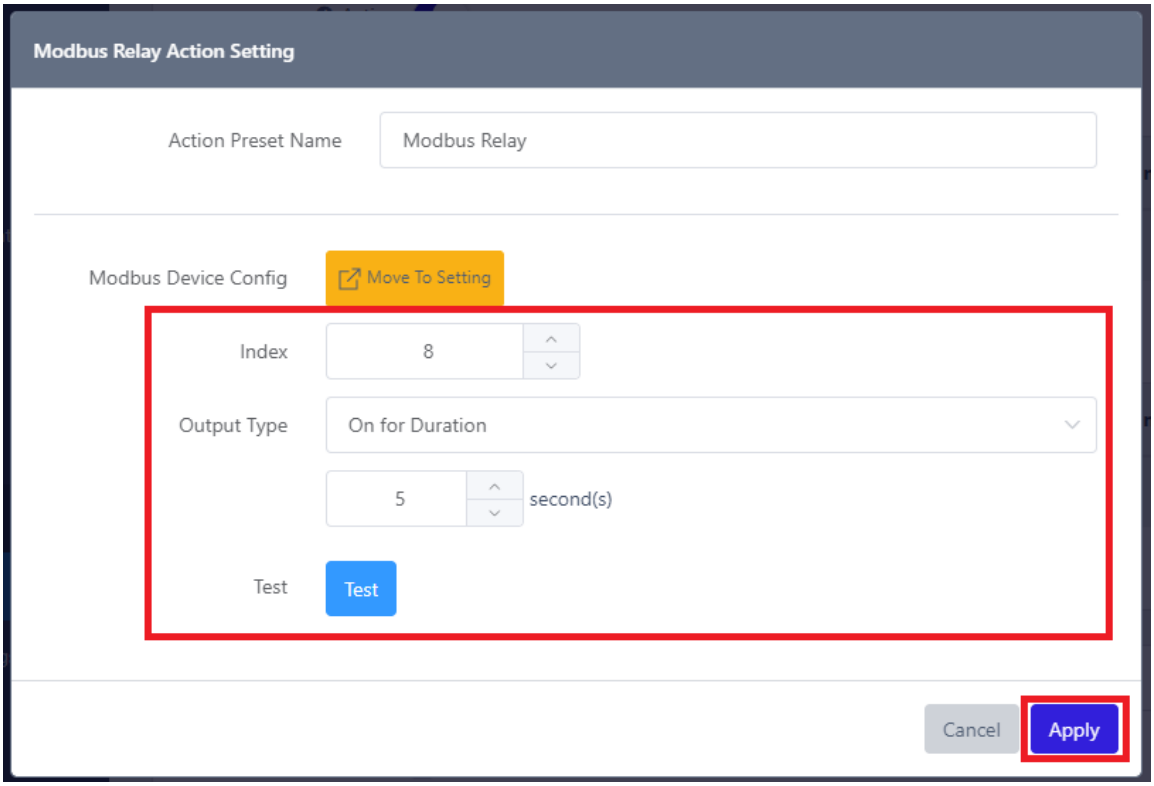
Select Modbus Relay from the Action Type.



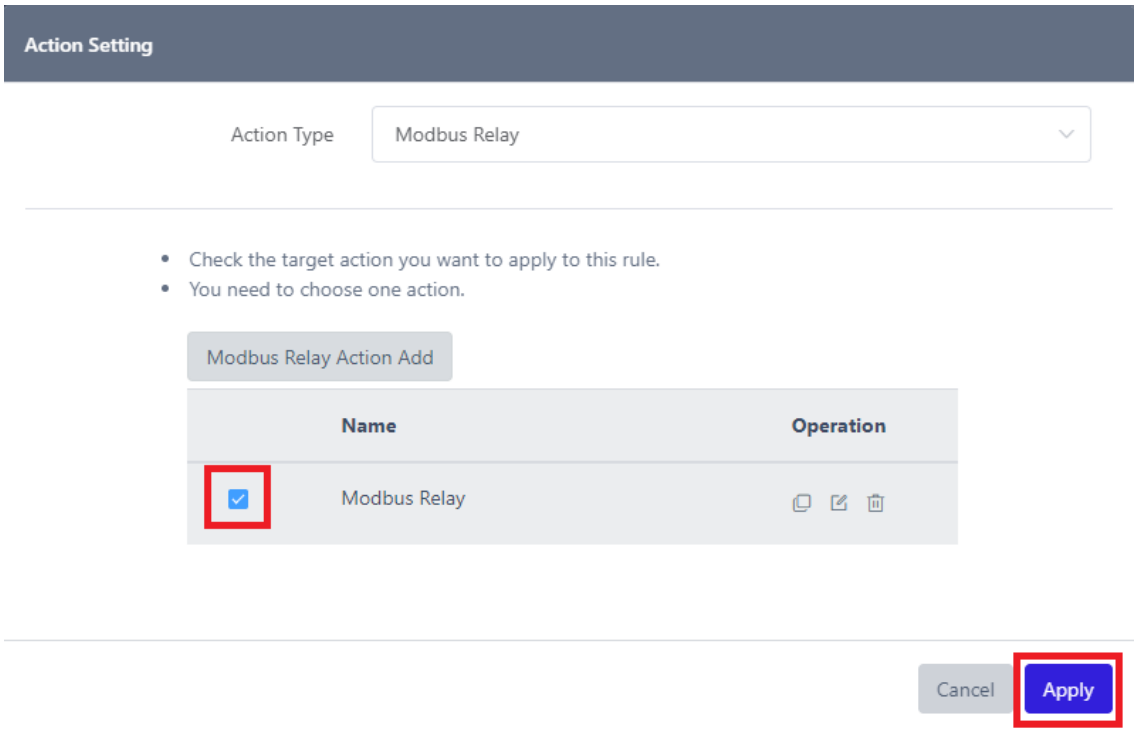
Clicked ‘Modbus Relay Action Add’ Button.



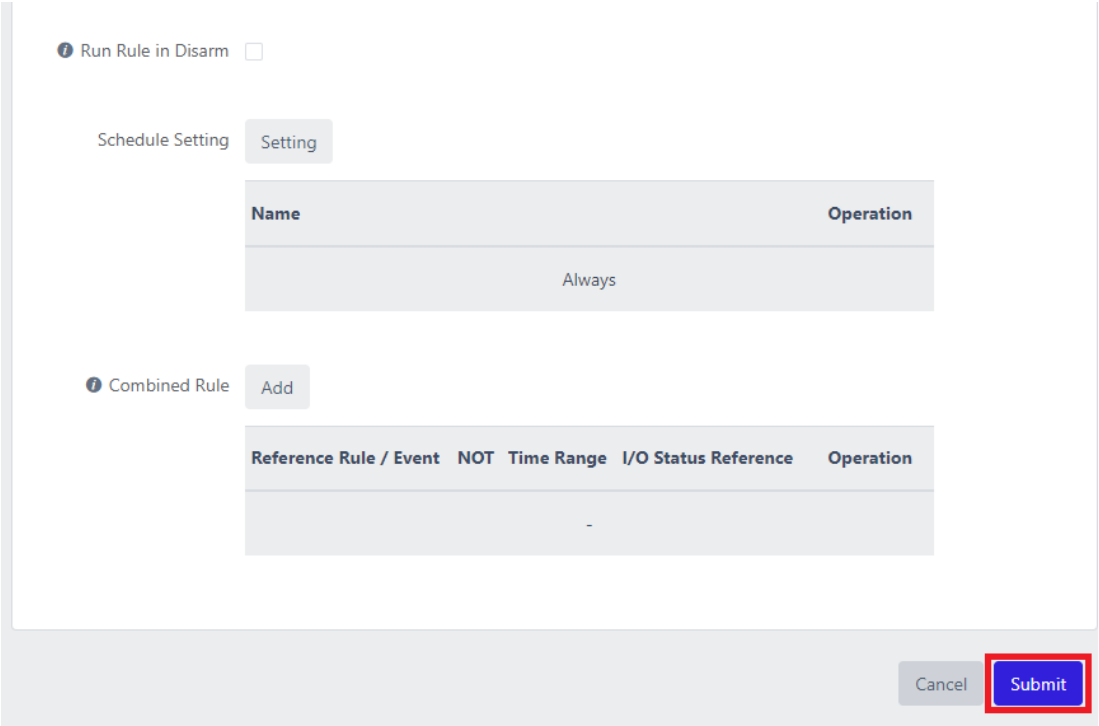
The Index refers to which Relay of the Relay device set in section 2.2.1 you want to control. Select the desired Output Type, then click the Test button to verify its proper operation. Finally, click the Apply button to save the settings.



Check the checkbox, then click the Apply button.



After completing the settings, click the Submit button to apply the changes.



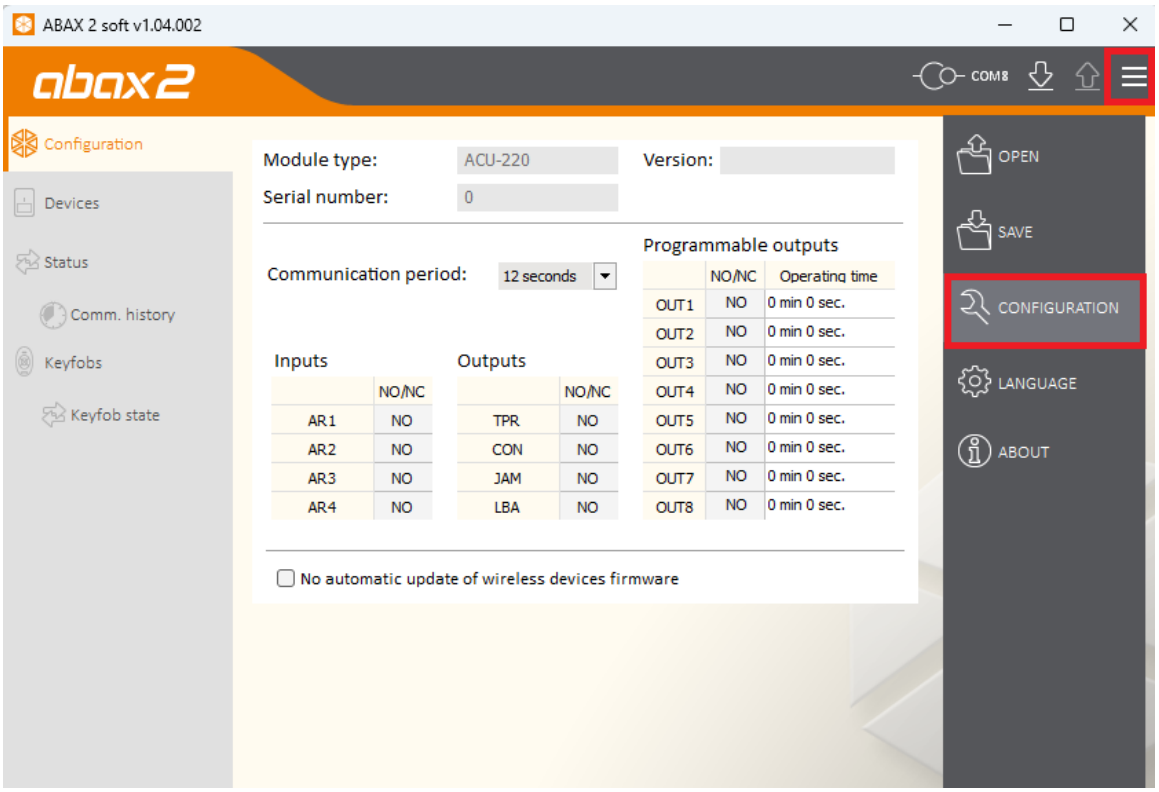
3. FAQ

3.1 ACU-220 Device Setting

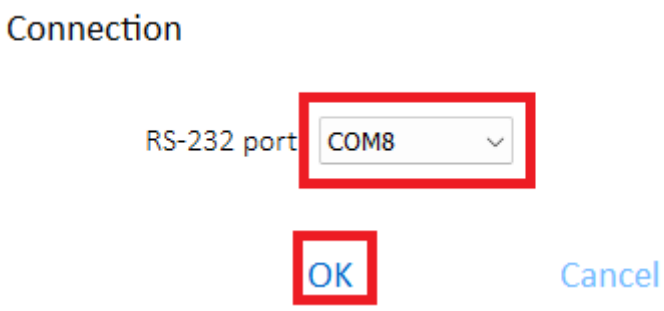
3.1.1 Connecting the ACU-220 to the PC (RS232)

Connect the RS232 to the PC connector provided by SATEL to the ACU-220, and connect the opposite USB to the PC. Then, run ABAX2.

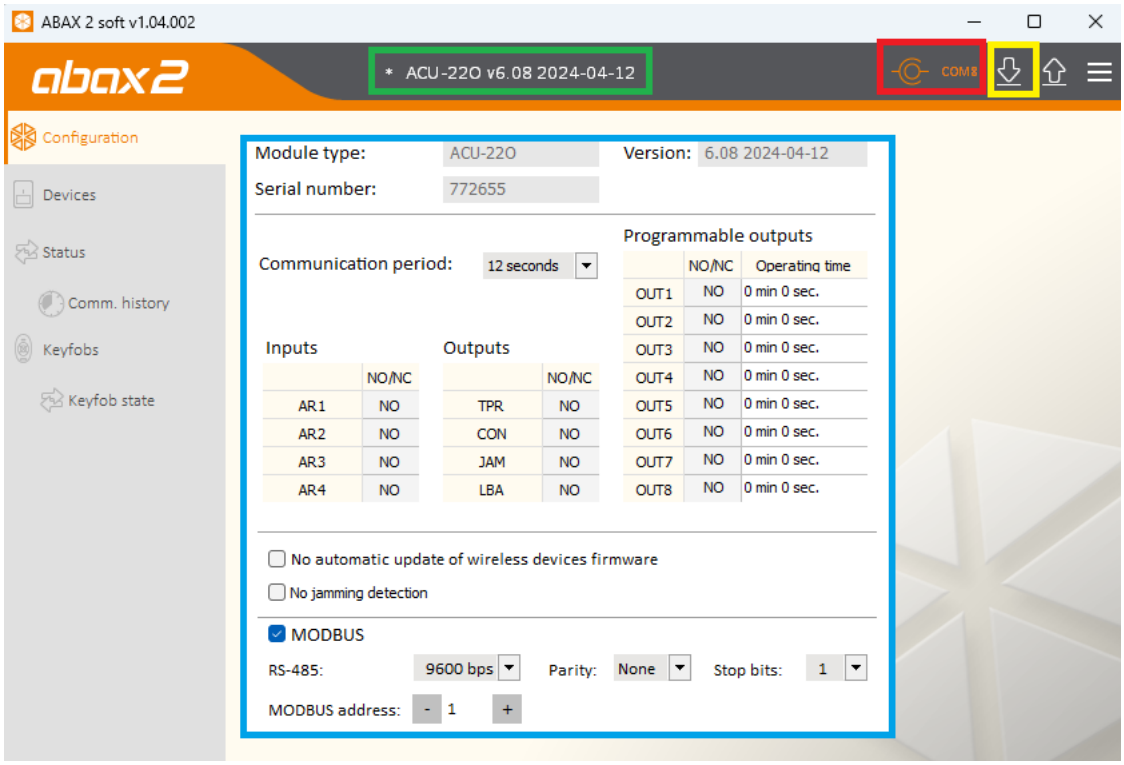
Click the menu button in the top-right corner (three horizontal lines), then click “CONFIGURATION.”



Select the port and click the “OK” button.



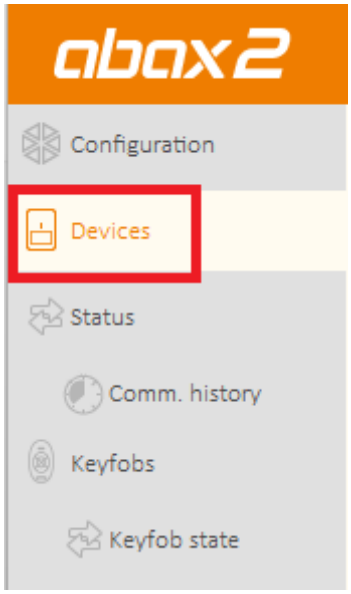
Click the button marked with a red box( ) in the top-right corner to successfully connect to the ACU-220. Once the connection is successfully made, the model name and firmware version will appear in the green box at the top center, and the asterisk (*) next to the model name will blink. Additionally, the current status of the ACU-220 can be seen in the blue box.



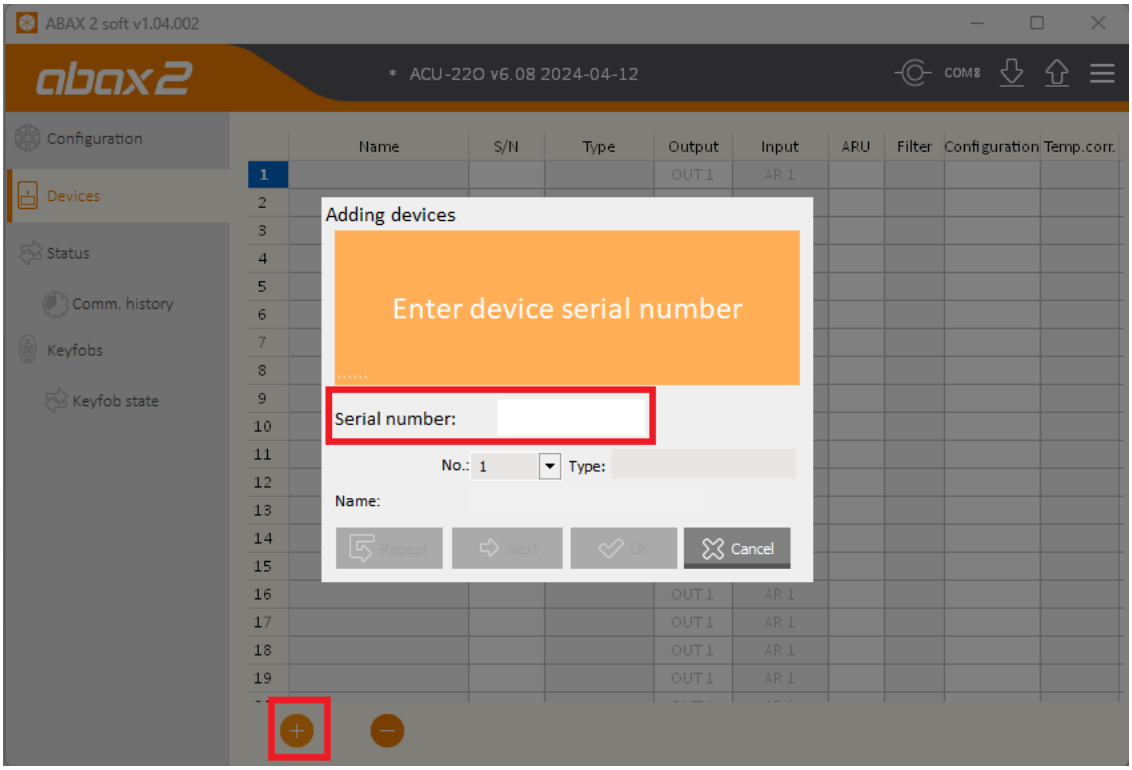
Tip. If you have just connected the ACU-220 or if a specific information box is highlighted in red, click the button marked with a yellow box( ) in the top-right corner to fetch the current status of the ACU-220.

3.1.2 Register a wireless device in the ACU-220

Click “Devices” in the left menu of ABAX 2.

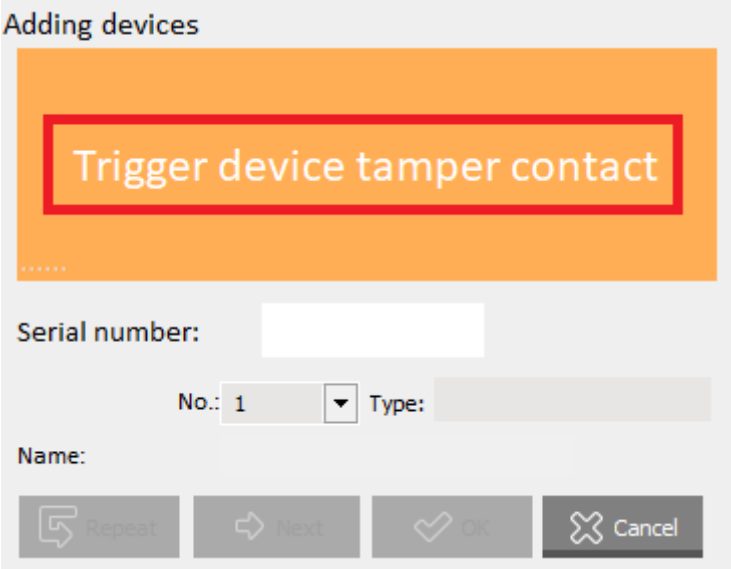


Click the button( ) at the bottom and enter the Serial number of the device to be connected. This manual is written based on the ACX-210.

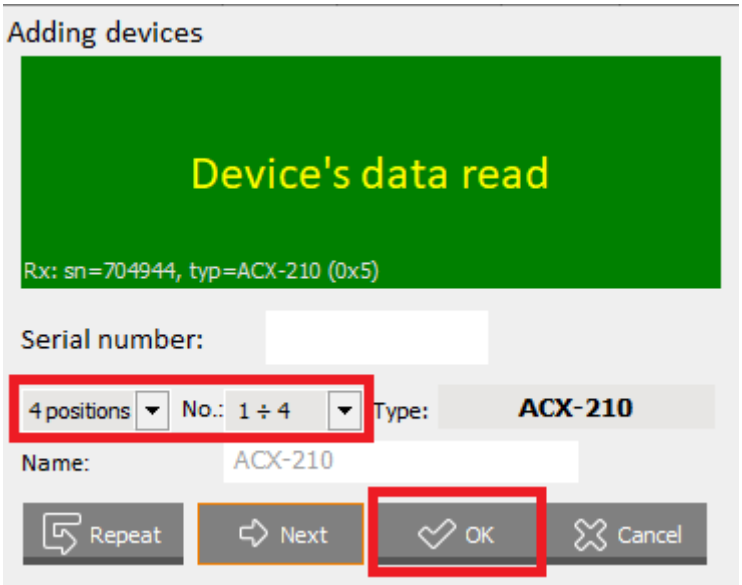


Tip. The Serial Number of the device is marked on the device as “sn:” and consists of 6 digits.

When you enter the Serial number, a message saying “Trigger device tamper contact” will appear as shown below.

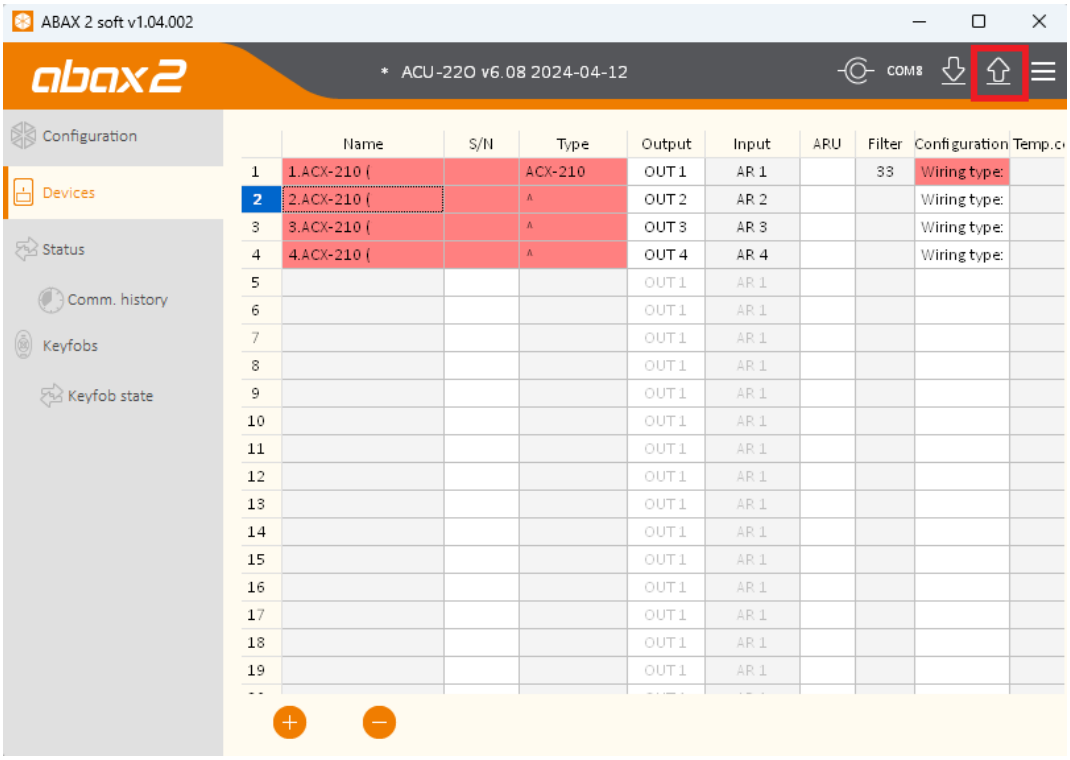


At this point, please power on the ACX-210. The device will then be recognized, and the screen will change as shown below. Select how many outputs you want to use, choose the position to list them, and then click the "OK" button.



Note. If only one position is selected, the outputs will be selected sequentially starting from position 1.

If the device is successfully added, click the button in the top-right corner ( ) to save.



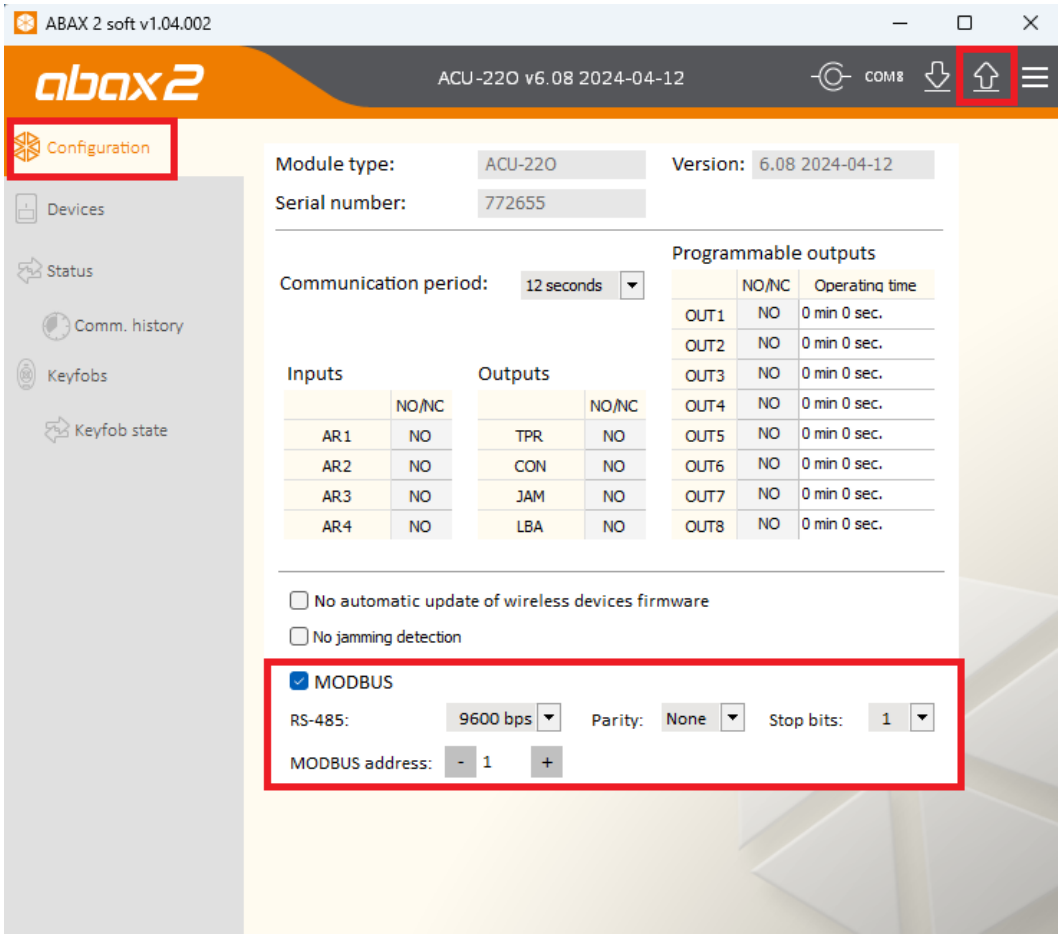
If the save is successful, the red box will disappear.

	Name	S/N	Type	Output	Input	ARU	Filter	Configuration	Temp
1	1.ACX-210 (		ACX-210	OUT 1	AR 1		33	Wiring type:	
2	2.ACX-210 (		^	OUT 2	AR 2			Wiring type:	
3	3.ACX-210 (		^	OUT 3	AR 3			Wiring type:	
4	4.ACX-210 (		^	OUT 4	AR 4			Wiring type:	
5				OUT 1	AR 1				

Note. The ^ symbol in the Type indicates that it is the same as the above content.

3.1.3 ACU-220 Modbus settings

In the Configuration tab of ABAX2, check the MODBUS settings at the bottom and select the desired configuration values. Once the settings are complete, click the button( ) in the top-right corner to save.



Tip. The Baudrate of the AIBOX is from 9600 to 115200 bps.

Note. The values set here are used in the AIBOX. The MODBUS address refers to the Device Address in the AIBOX.

TCP Modbus (WAVESHARE)

1. Introduction

1.1 Prerequisites

- AIBOX FW version 103719 or higher.
- TCP Modbus Relay Box

Recommended Alarm Box models:

- Waveshare Modbus POE ETH Relay
- Waveshare Modbus POE ETH Relay (B)
- Waveshare Modbus POE ETH Relay 30CH

1.2 Learn about integration architecture

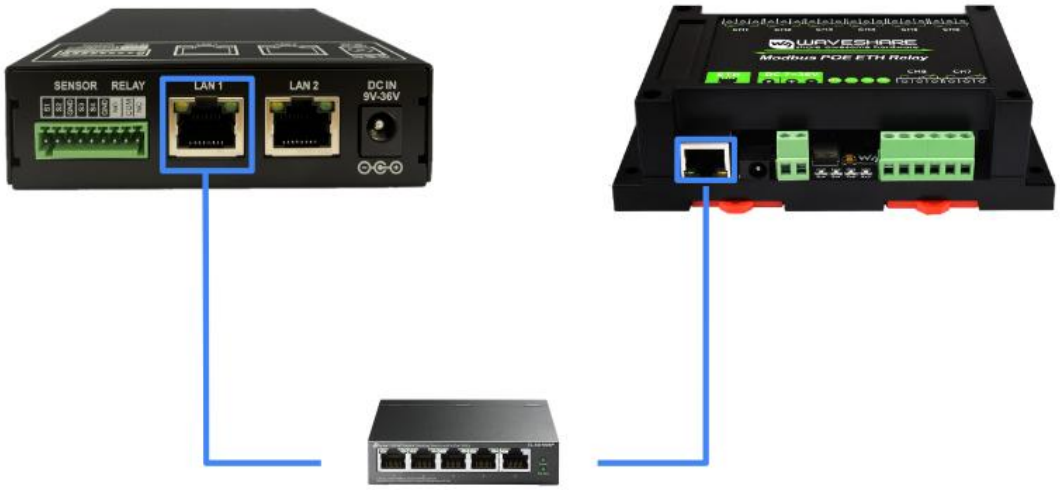
There are two ways to integrate AIBOX out of Alarm Box (Modbus POE ETH Relay) :

1) Case 1 : **Direct LAN2 Connection with AIBOX**

You will connect the Waveshare Modbus POE ETH Relay (hereinafter “Relay”) to the LAN2 port of the AIBOX. You must assign an IP address to LAN2 on the AIBOX, and the Relay needs to be powered. You will need to use a POE injector or supply external power to the Relay. If you assign the LAN2 IP address of the AIBOX to 192.168.1.xxx, there’s no need to configure the IP on the Relay, as the default IP of the Relay is 192.168.1.200.

2) Case 2 : **LAN1 Connection via Switch (Non-Recommended)**

In this case, you will connect the Relay to the LAN1 port. This setup requires configuring a switch. If the switch does not support Power over Ethernet (POE), you will need to supply additional power to the Relay and change its IP address. **However, since Modbus TCP does not include any built-in authentication mechanisms, this method is not recommended due to potential security risks, as unauthorized access to the Relay could occur on the network**



2. Configuration

To integrate the AIBOX with the Waveshare Modbus POE ETH Relay, each device must be configured properly. Below are the steps for configuration, based on **Case 1**. If you prefer **Case 2**, refer to section 3.1 for additional settings required for the Waveshare Modbus POE ETH Relay.

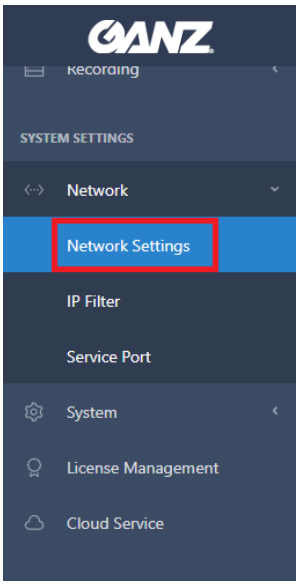
2.1 AIBOX

Here are the steps to configure the AIBOX for use with Modbus equipment.

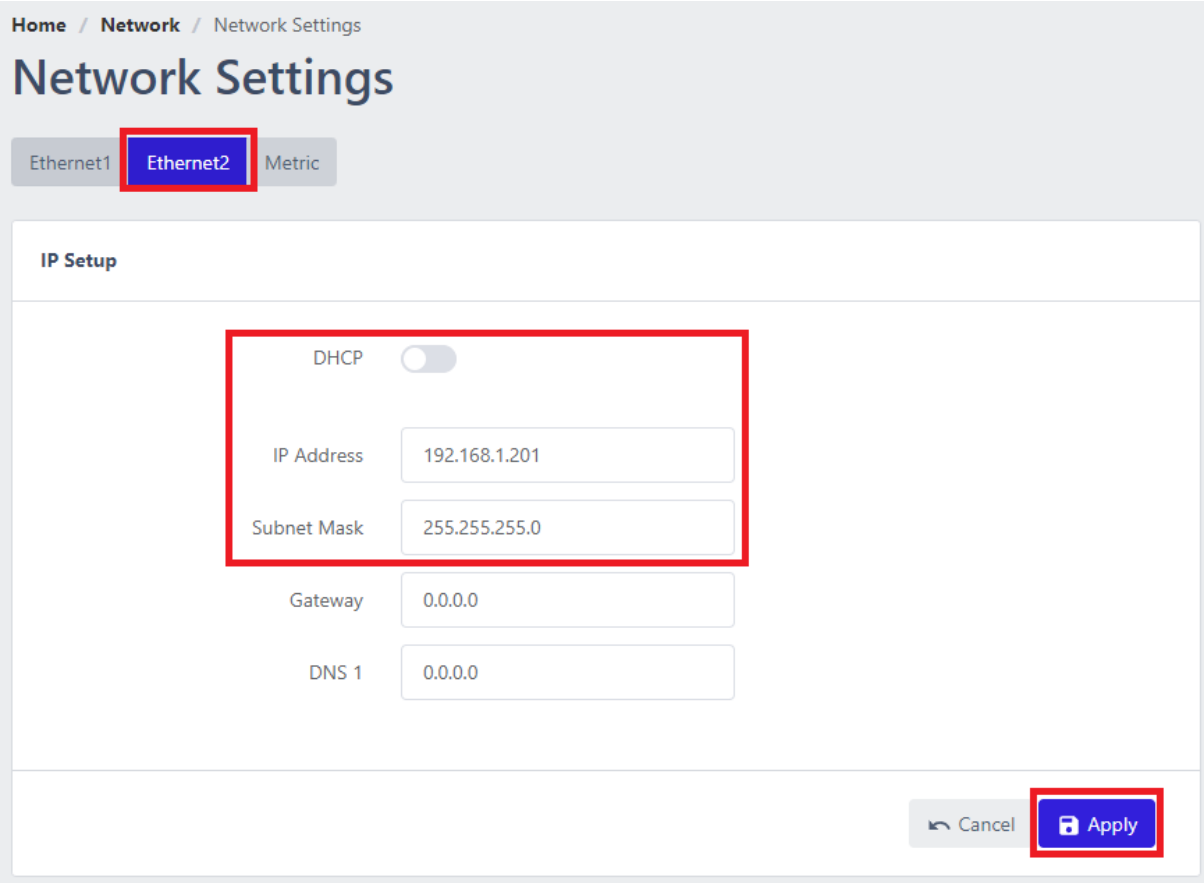
2.1.1 Network Setting

We recommend using Case 1, so you need to configure Ethernet2. Below are the instructions for setting up Ethernet2.

Access the AIBOX webpage and click on Network Setting under SYSTEM SETTING in the left menu bar.



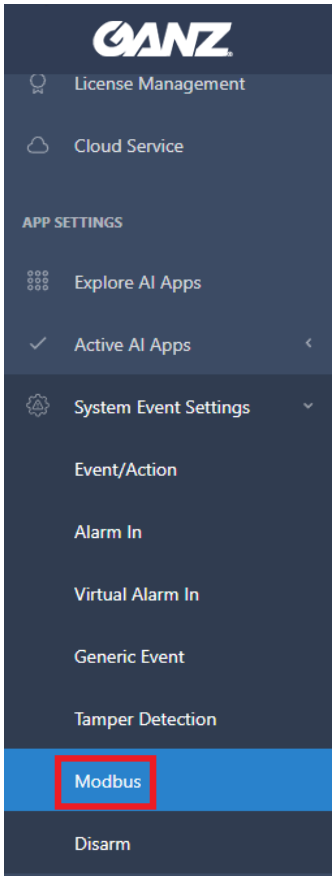
Click on Ethernet2, then turn off DHCP and configure the IP address and Subnet Mask.



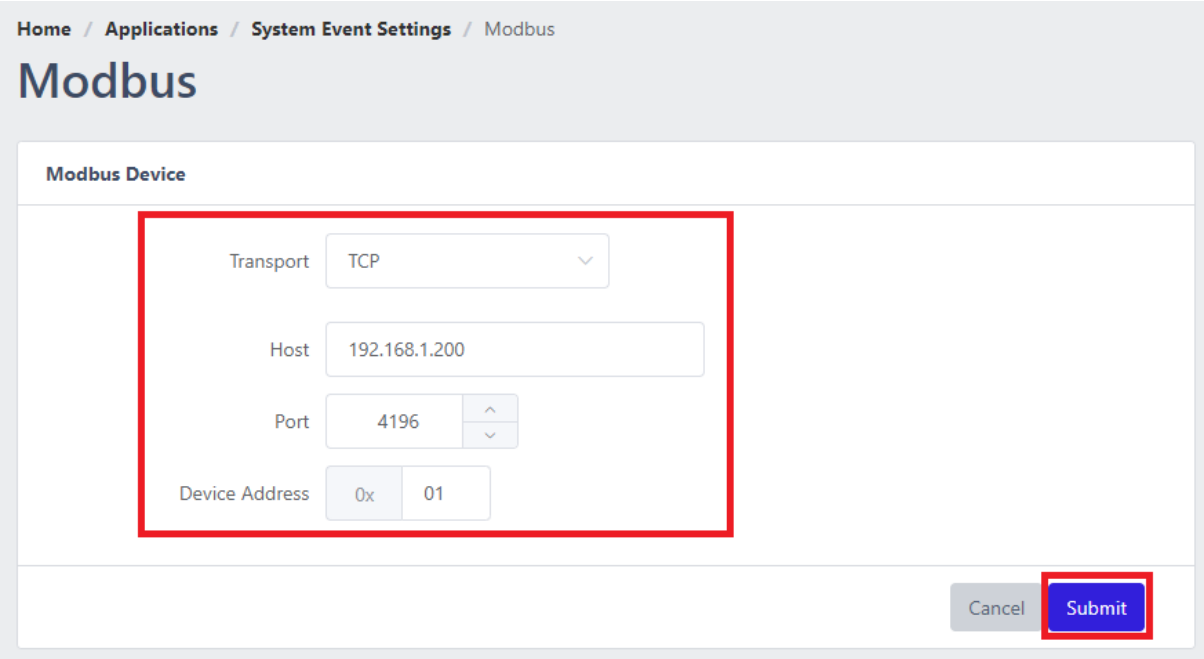
Note: If only the Relay device is connected to eth2, do not configure the gateway and dns1 settings.

2.1.2 Modbus Relay Setting

Access the webpage and select APP SETTING > System Event settings > Modbus from the left menu bar.

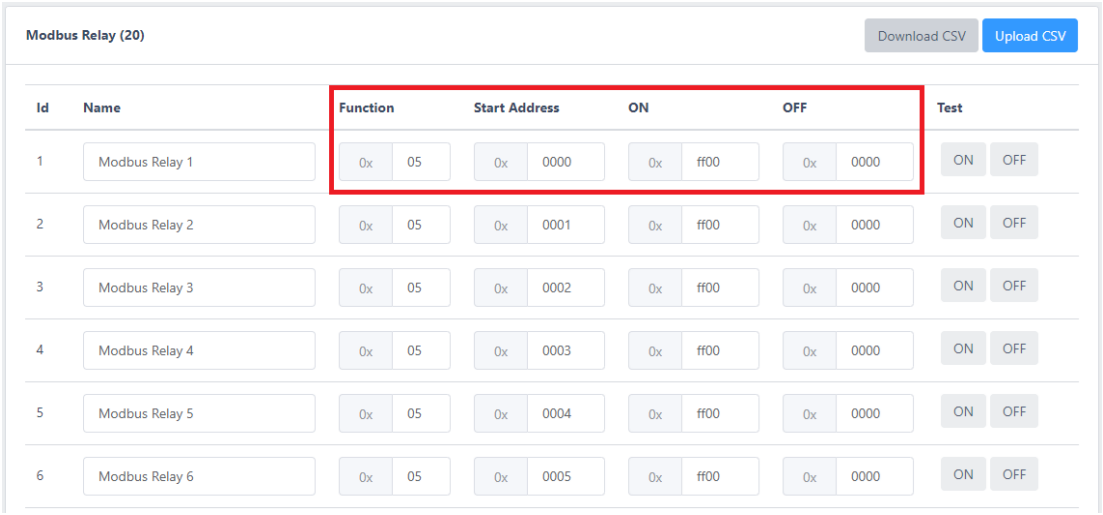


Select TCP for Transport and configure the Host and Port settings. For the Waveshare Modbus POE ETH Relay, the Device Address is fixed at 0x01.

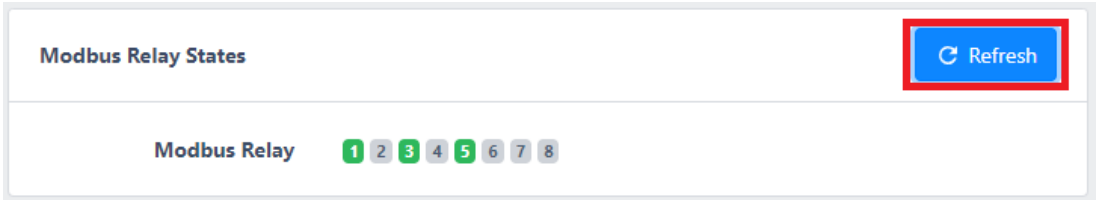


Note. The device's default IP is 192.168.1.200, and the port is 4196.

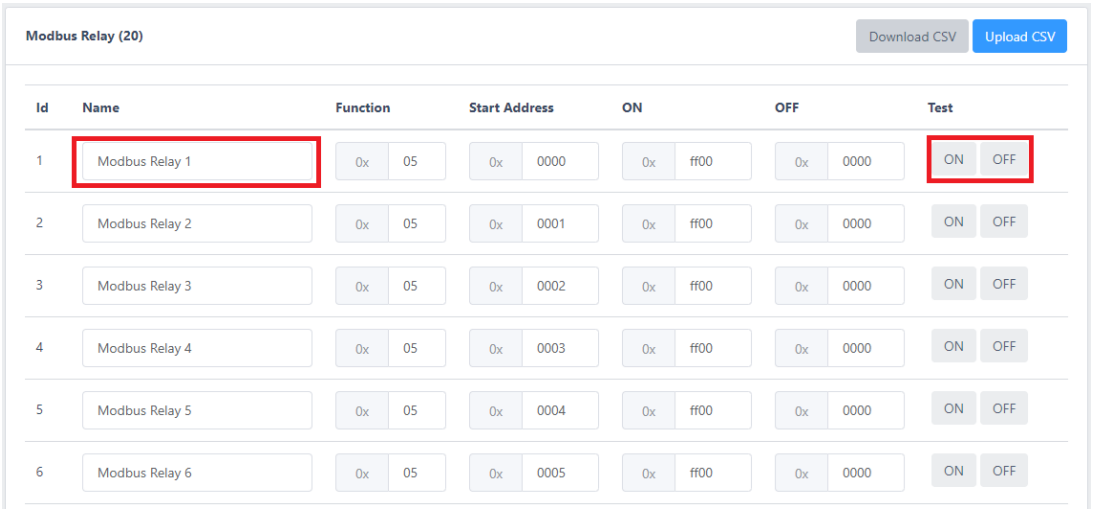
Enter the following configuration values: For the Waveshare Modbus POE ETH Relay, the Function is fixed at 0x05, the Start Address is 0x0000, ON is 0xff00, and OFF is 0x0000.



Tip. Click the Refresh button to check the current Relay status of the connected device.



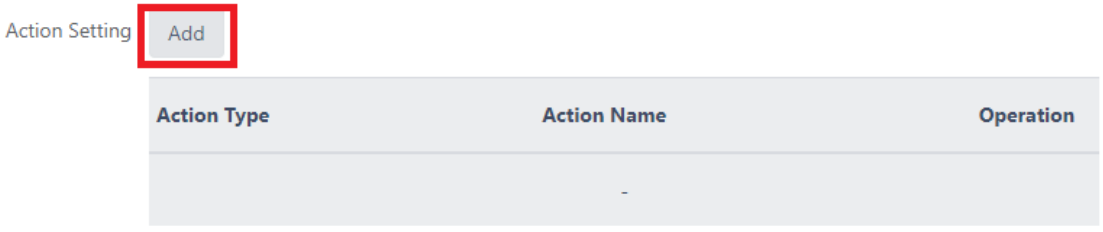
Tip. You can set the name of the Relay you wish to use and click the ON/OFF button to test it.



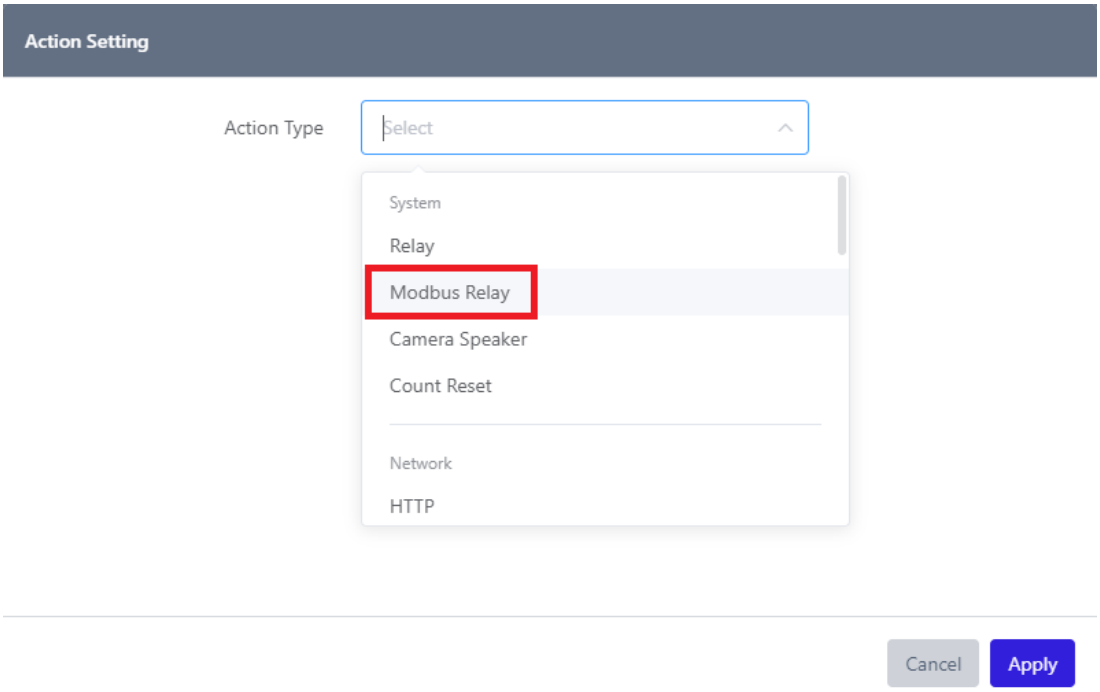
2.1.3 Modbus Relay action

Below are the instructions for adding the Relay device registered in the AIBOX to the action settings.

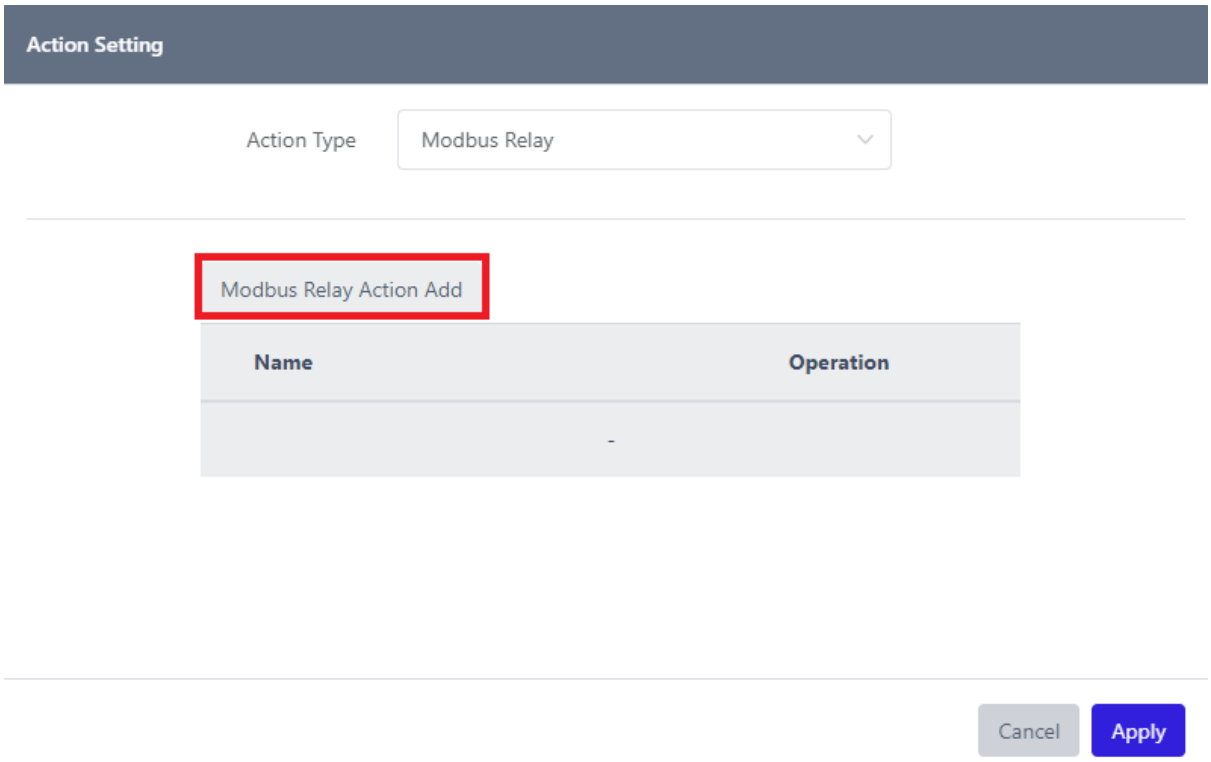
After setting up the AI App or system events, click on Action setting and then select Add.



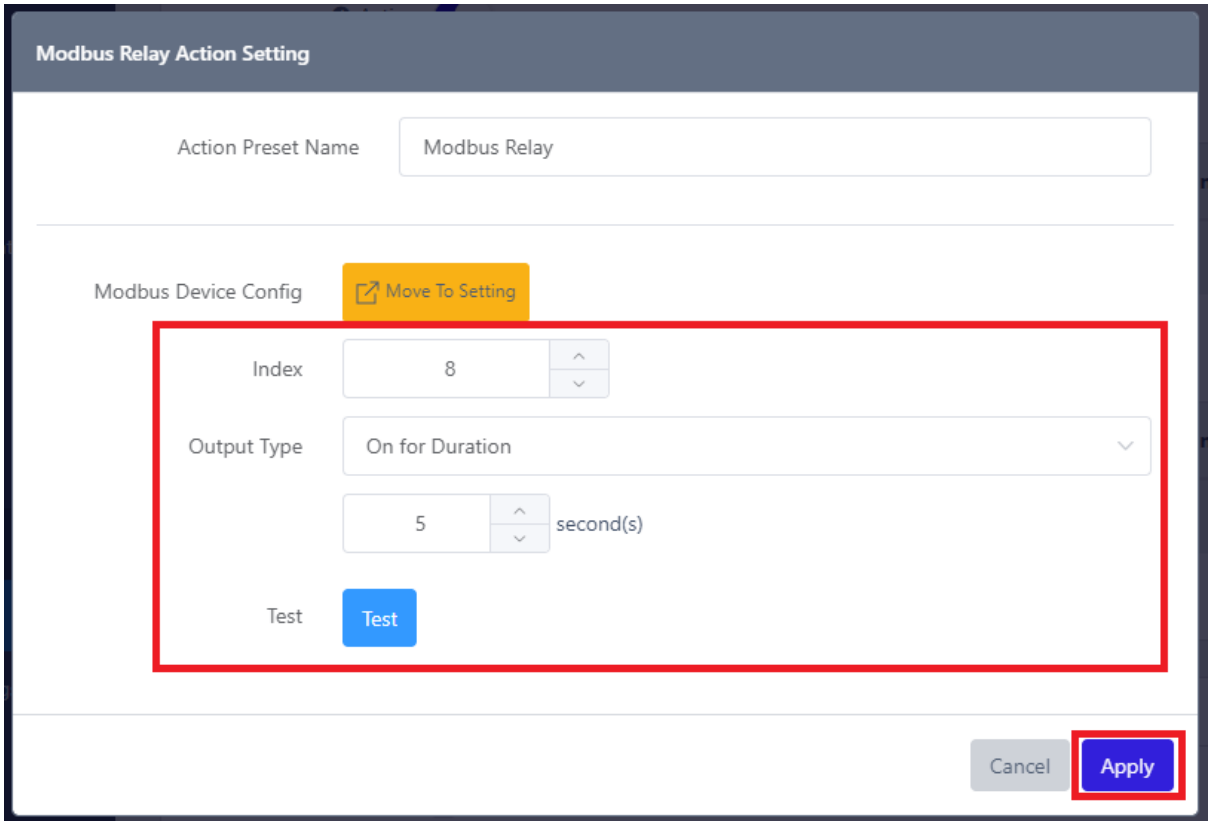
Select Modbus Relay from the Action Type.



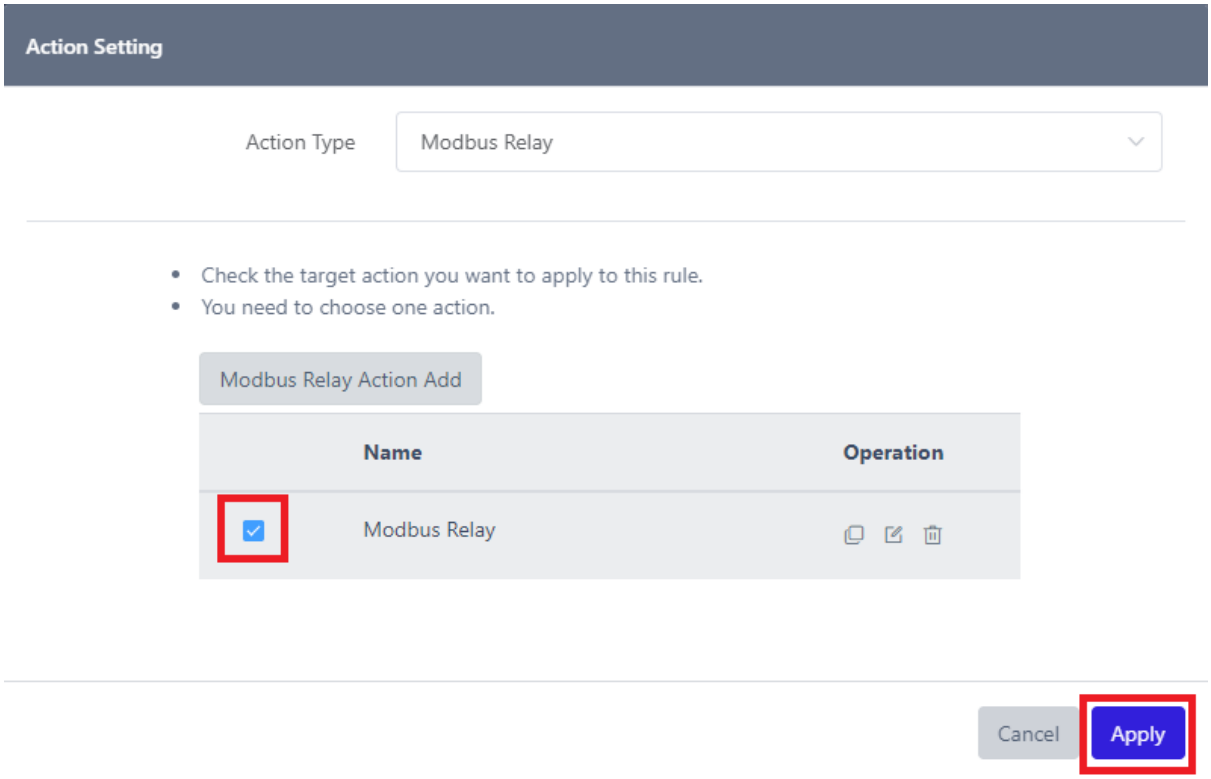
Clicked ‘Modbus Relay Action Add’ Button.



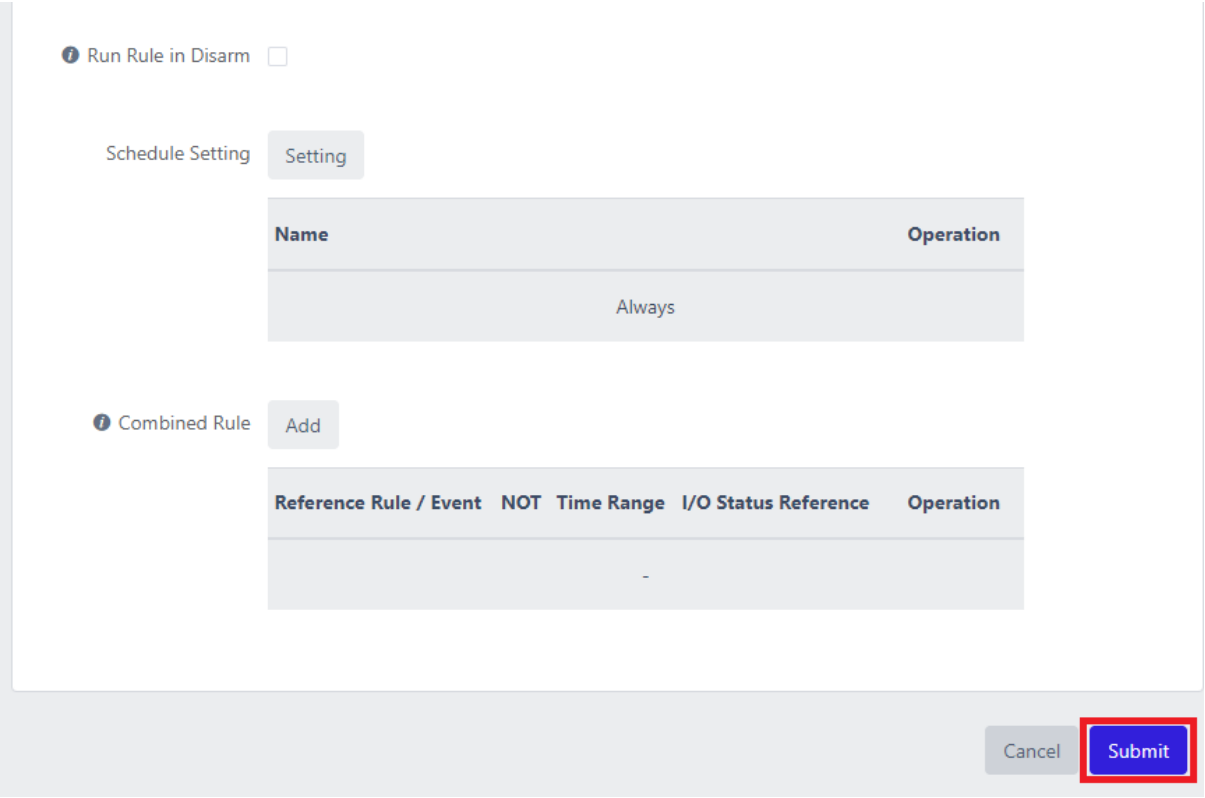
The Index refers to which Relay of the Relay device set in section 2.2.1 you want to control. Select the desired Output Type, then click the Test button to verify its proper operation. Finally, click the Apply button to save the settings.



Check the checkbox, then click the Apply button.



After completing the settings, click the Submit button to apply the changes.



3. FAQ

3.1 Waveshared Modbus POE ETH Relay Device Setting

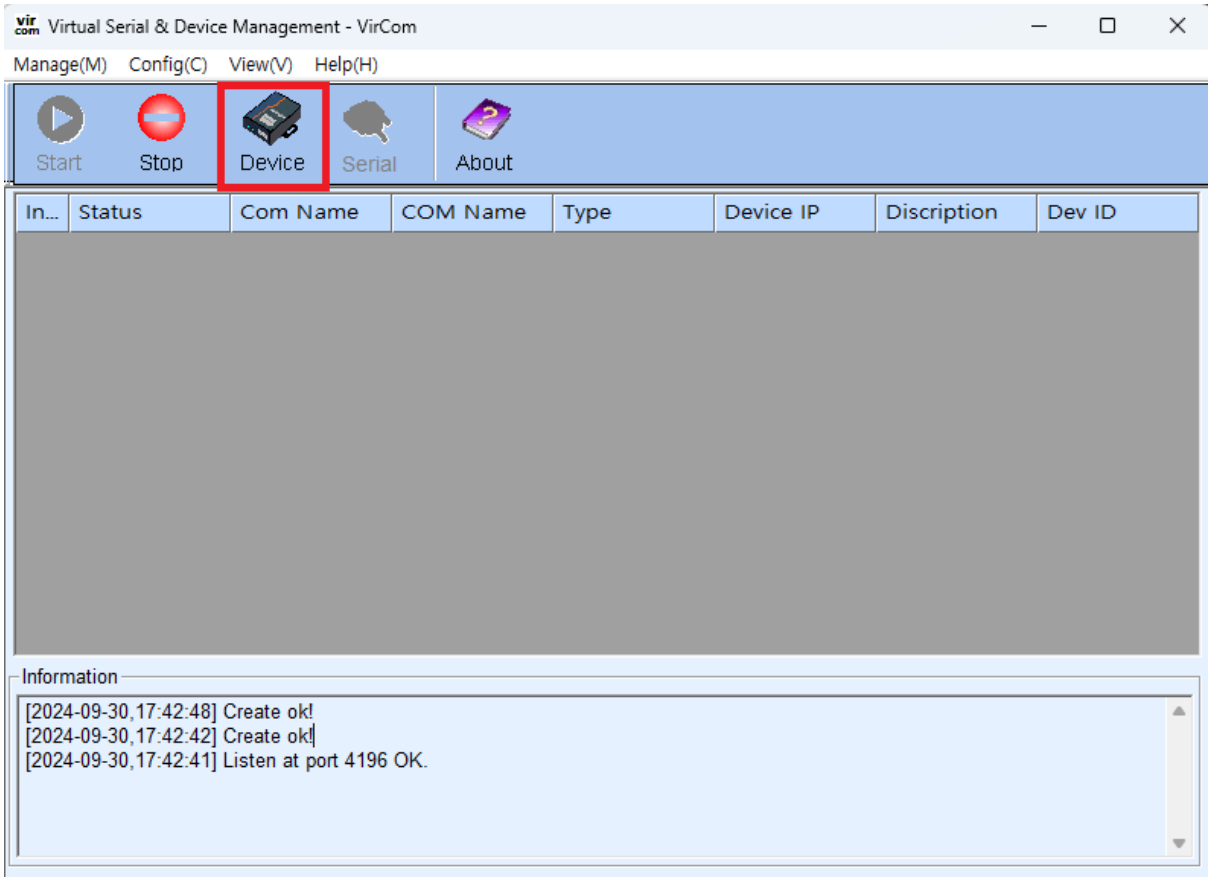
To locate and configure the device, please download the installation file provided below. The tool is a **zip** file containing a **Windows executable**.

VirCom Tool Download Link

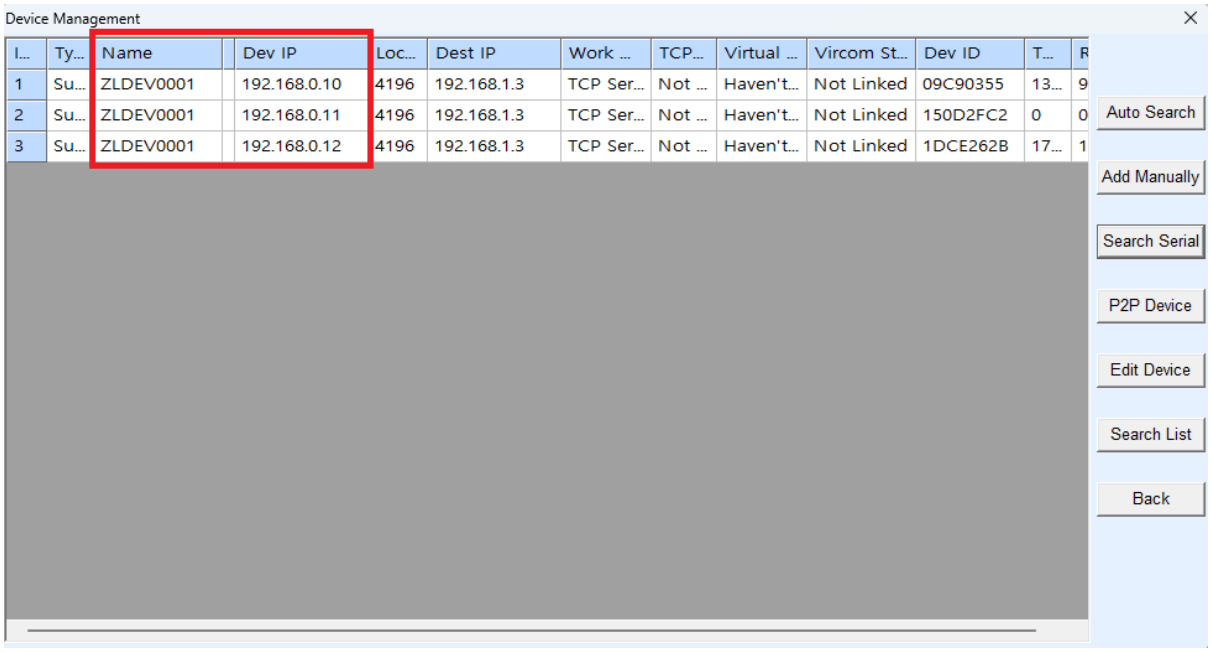
3.1.1 Search Device

On a Windows PC connected to the same network as the Relay device, download the VirCom tool, extract the compressed file, and run the tool.

Clicked the 'Device' Button

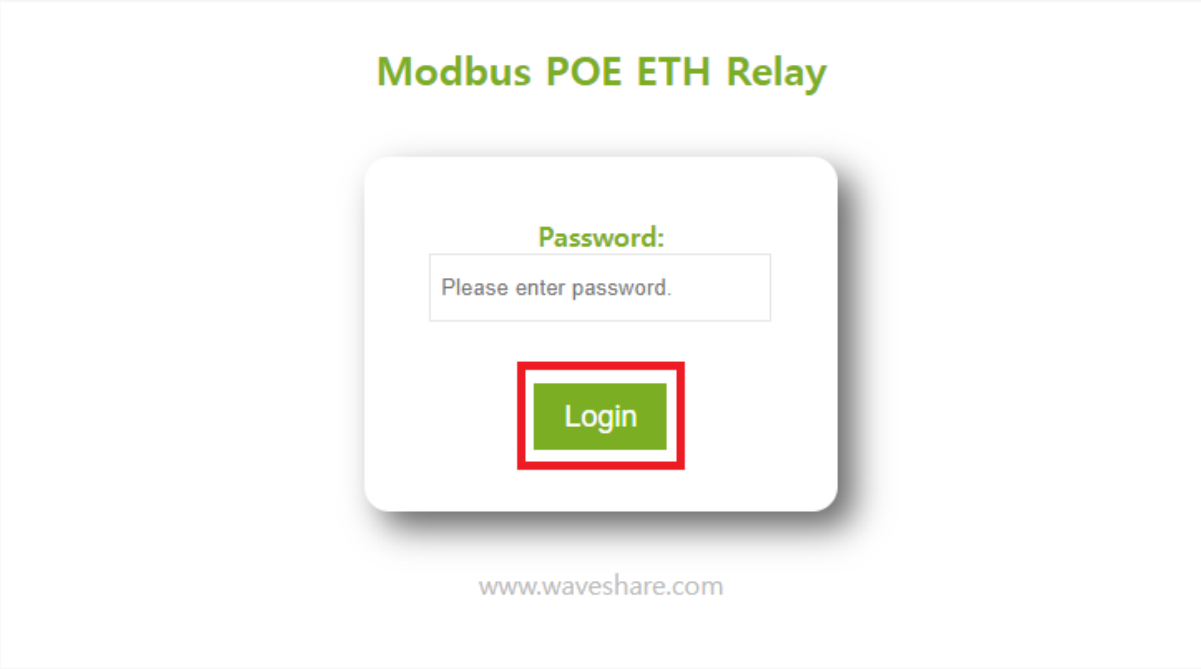


Devices on the same network will be detected. If a device is not found, please check the network connection and the power status of the device.



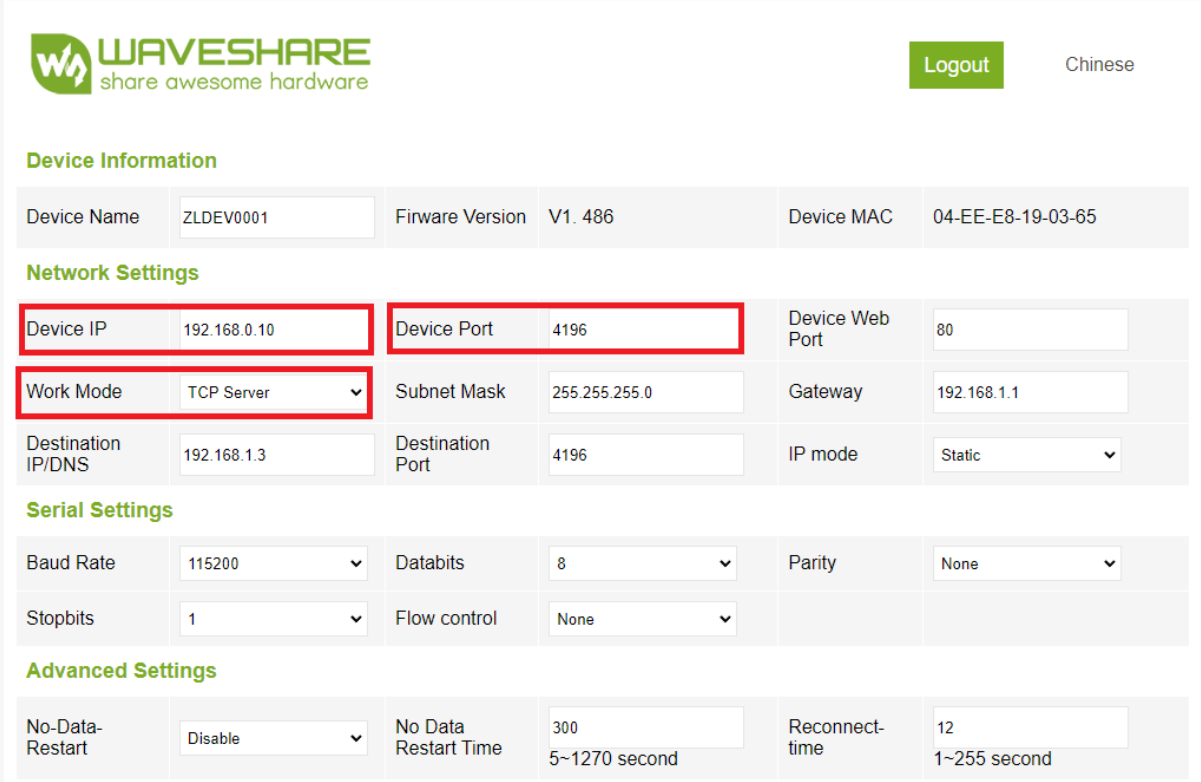
3.1.2 Configuration

Connect to the device you identified in section 3.1.1.



Note. The device has no default password. You can enter any value or leave it blank to log in.

Set the device's IP and port, and configure the work mode as TCP Server.



Note. The device's default IP is 192.168.1.200, and the port is 4196.

Tip. When setting up multiple devices, ensure that you configure each device **one at a time**. Since all devices start with the same default IP address, configuring multiple devices simultaneously may cause conflicts, and changing the settings for one device could inadvertently affect the others. To avoid this, always complete the configuration of one device before moving on to the next.

Network Action Handler

HTTP

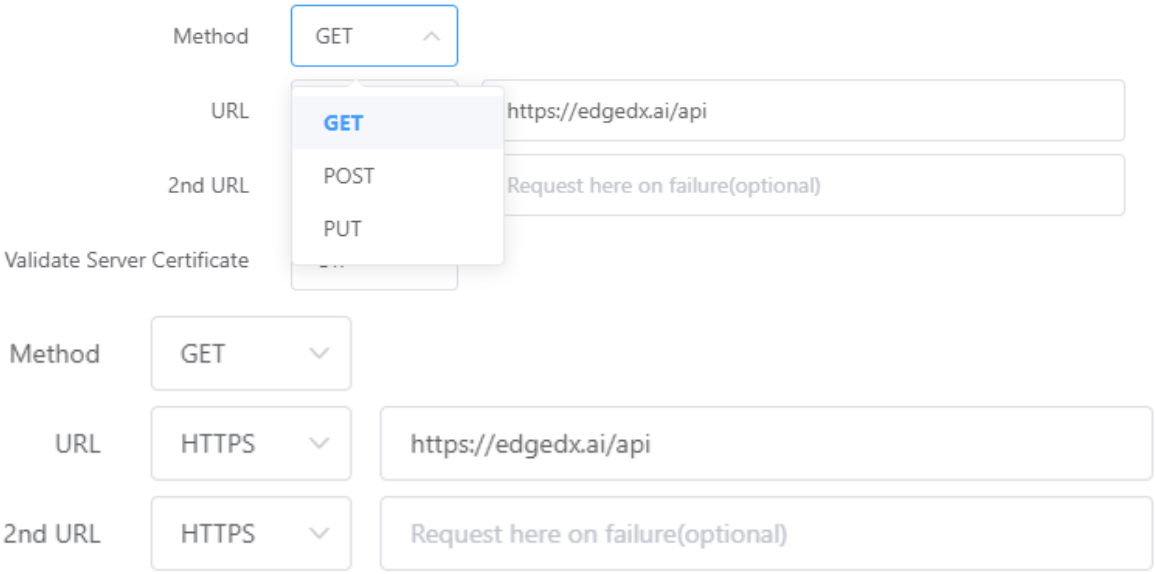
When an event occurs, the device can upload event information and snapshot images to an external HTTP server.

Messages to be uploaded can be easily edited using token variables.

Select the Action Type to **HTTP**, then the relevant settings at the bottom

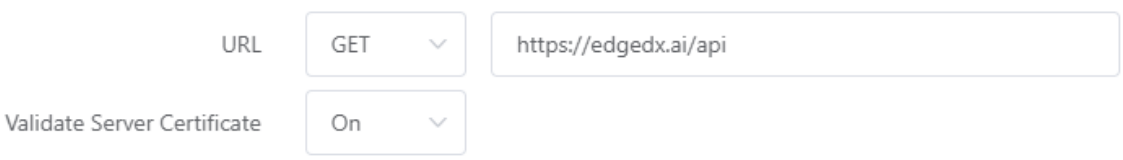
1. URL Settings

1. Select the HTTP API URL and Method.

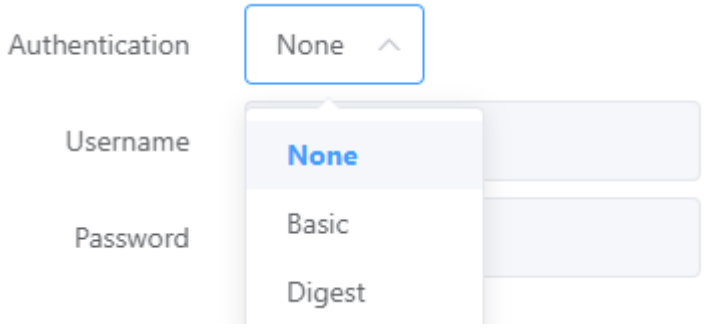


- 2nd URL :If you configure a 2nd URL, the request to the 2nd URL is automatically retried only if the request to the primary URL fails.
  However, if the request to the primary URL is successful, the request to the secondary URL will not be made.
  The 2nd URL is not a required value, so you do not have to set it

2. If you input **Https** protocols, the Validate Server Certificate is activated.

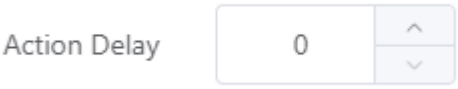


2. Authentication



Authentication methods are available None, Basic, and Digest.

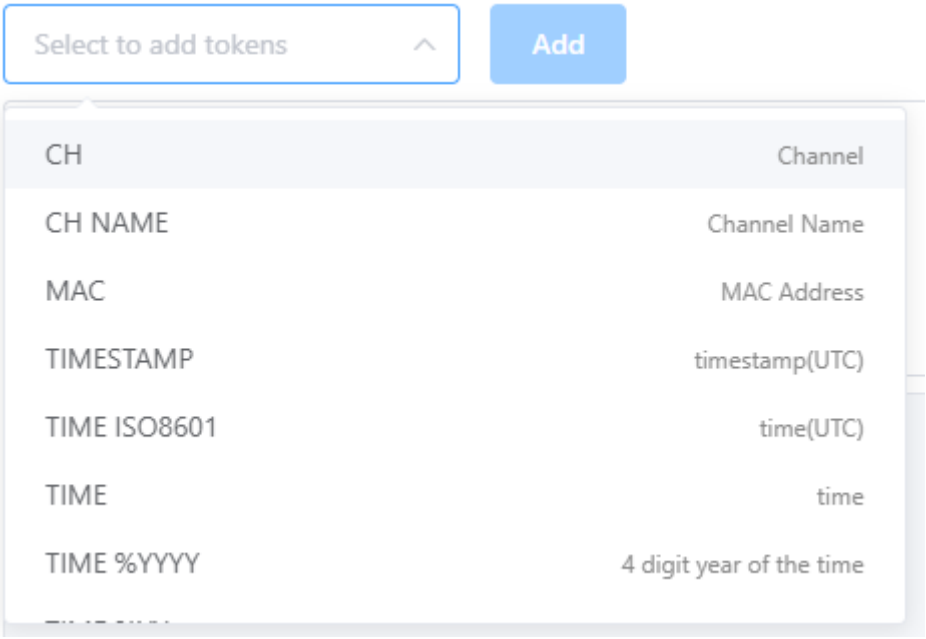
3. Action Delay



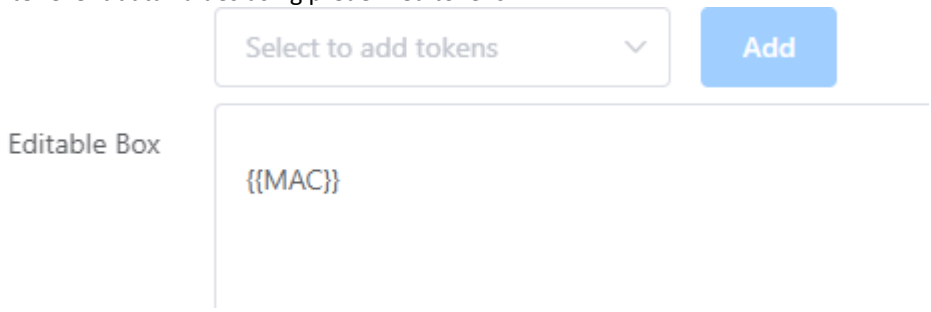
After the event occurs, the message is sent after a delay of the amount of time specified in Action Delay. Normally, you can leave it at the default value of 0.

4. Show event data

API request data can contain event information.



1. Enter event data values using predefined tokens.

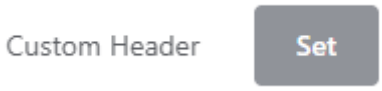


2. Select the desired token value from the combo box.
    - The selected token value will be added as {{token}} in the form of {{token}}.
    - When sending actual data, this part is replaced by event data.
    - Tokens can only be used where they can be input via the combo box.

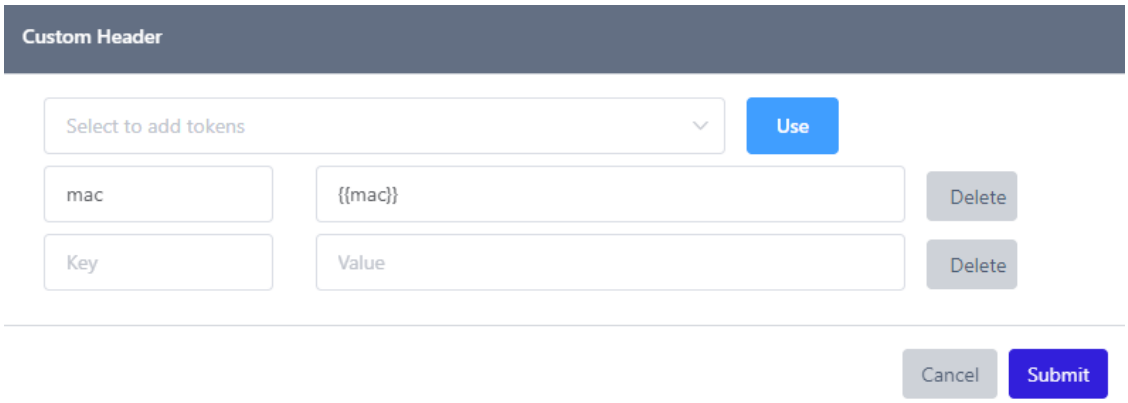
5. Custom Header Settings

1. Click the 

button to set the header



2. You can use event data tokens on the Custom Header settings page. To use a token, select the text field and add the token. It is only available for Value.



3.

6. Query Settings

The query string can be configured in the same way as the header.
Once set, you will see a quick view of the query string.

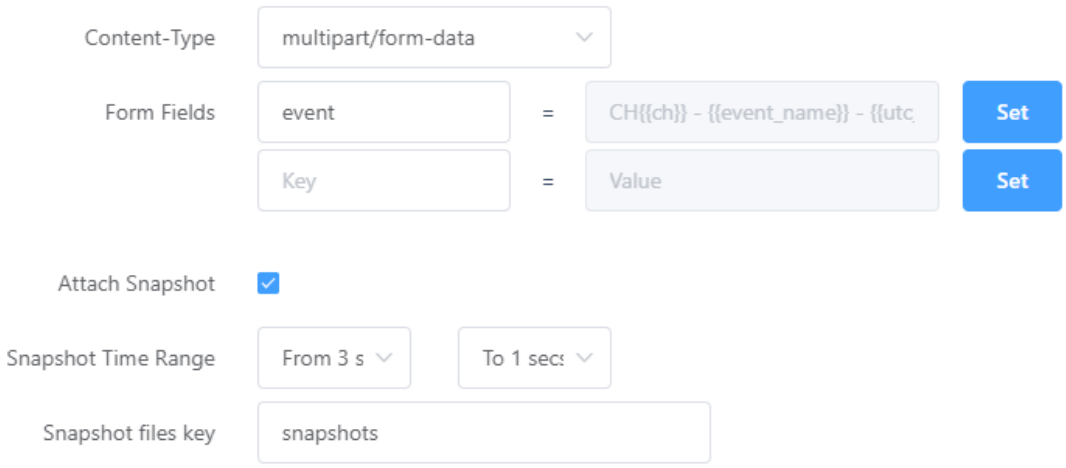
7. Content-type

Selecting Content Type will display the Type settings page.

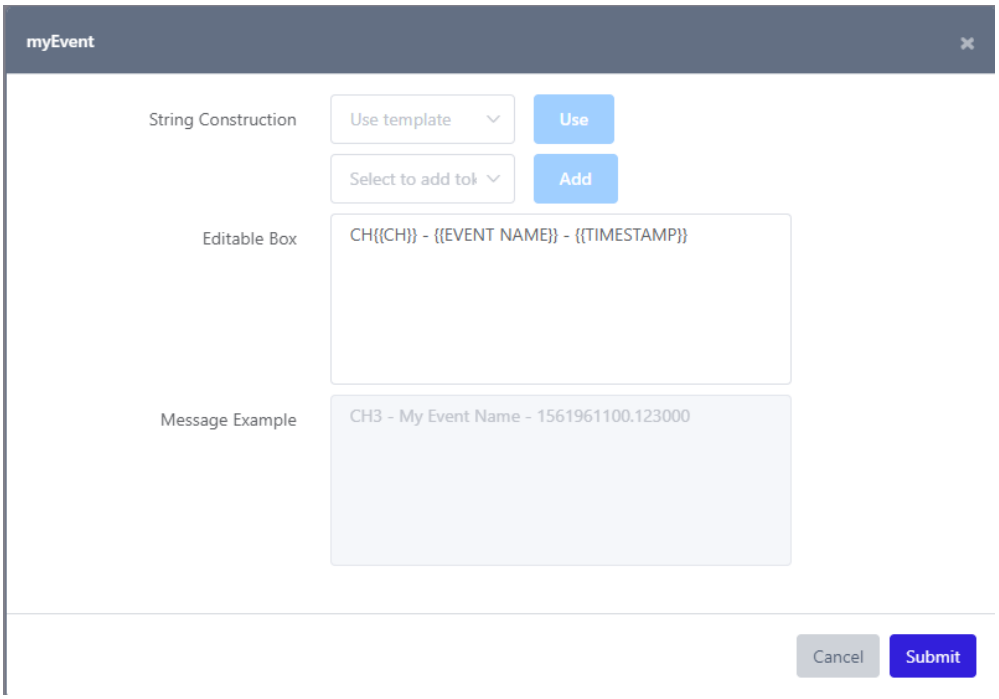
Content-type : multipart/form-data

From Field Settings

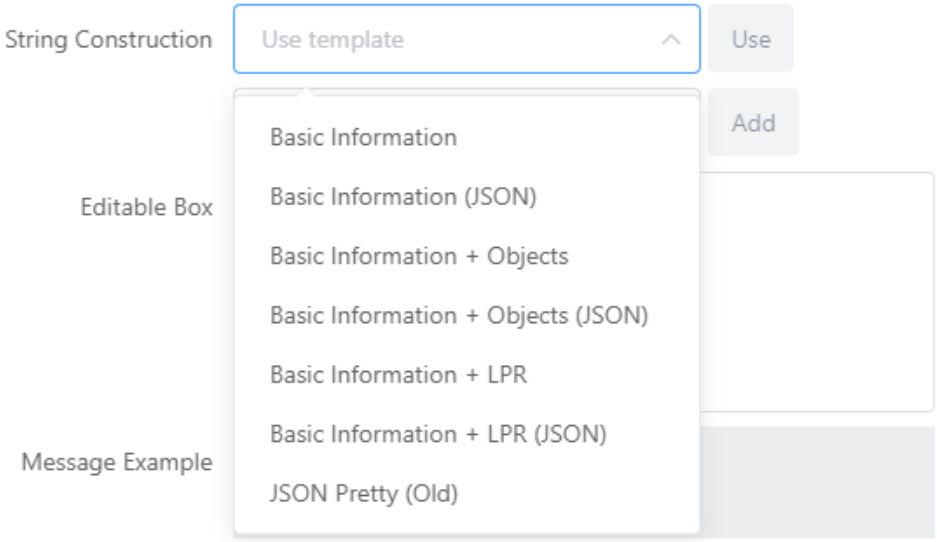
1. Click the Set button to set the data.



2. If you click the Set button, the settings window pop-upUse the event data token to set the value. There's also a simple template.

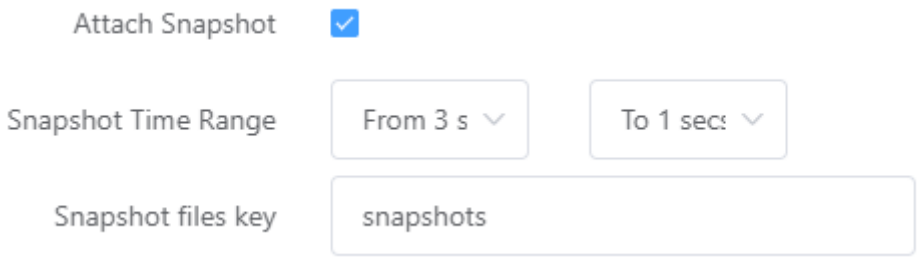


- There are also simple templates available.



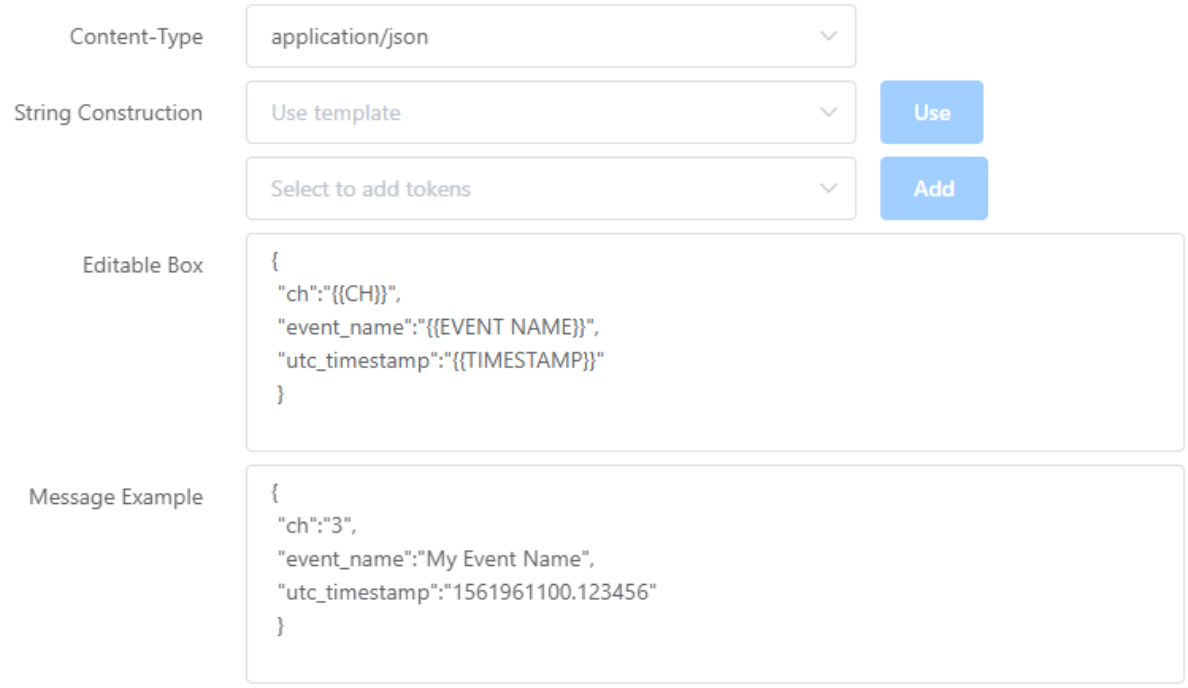
Snapshot settings

multipart/form-data allows snapshots to be appended.



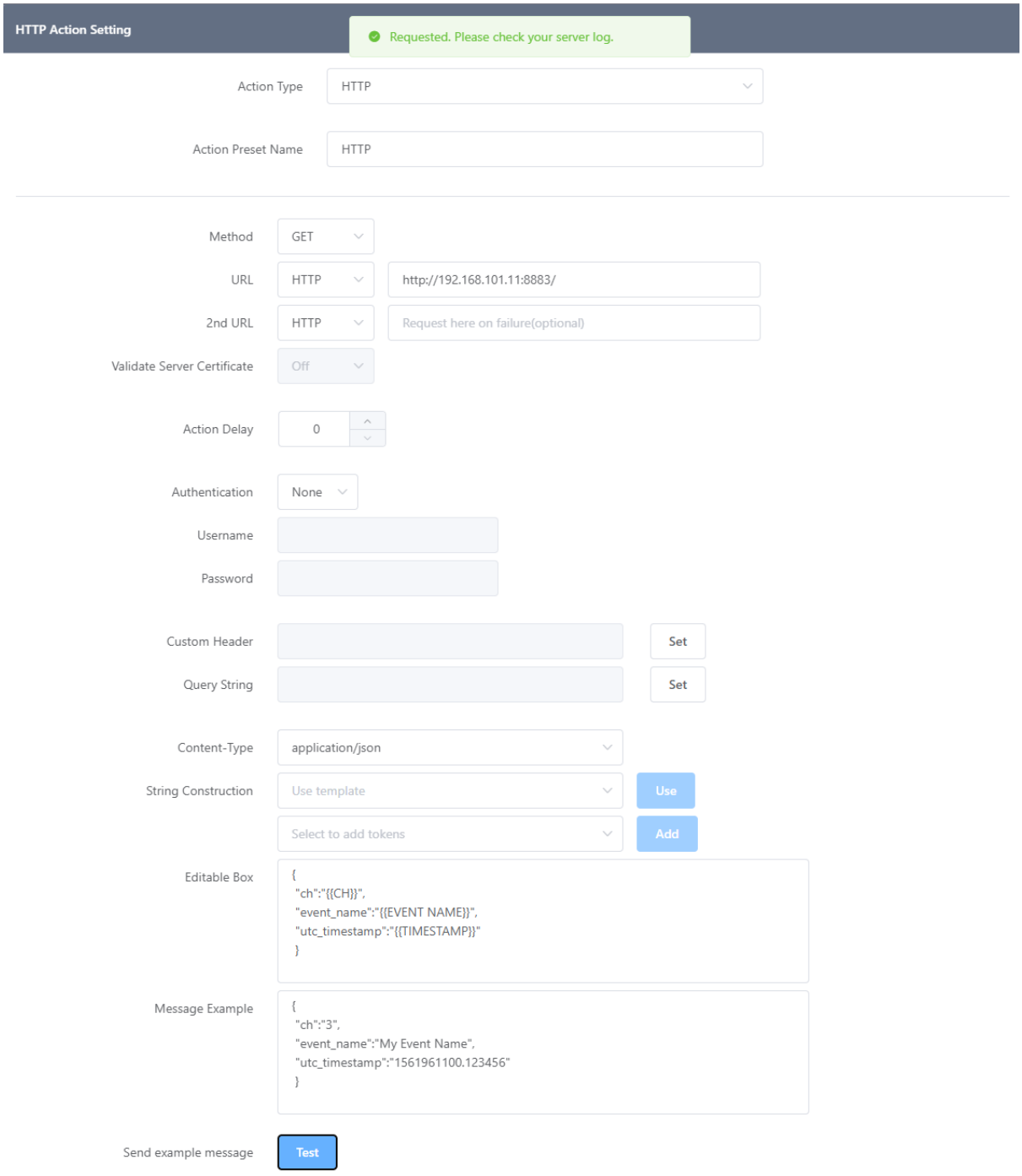
Content-type: Application/Json

Application/Json provides event data token functionality and template functionality.
It also provides templates in the form of Json.



8. Message test

You can test your setup data using the Test button at the bottom.
Success is displayed at the top.



FTP Upload

FTP upload allows you to upload an event snapshot to an FTP server when an application event occurs. The directory and file name to store the snapshot file can be set variably using the event's metadata.

The FTP Upload can be added from the Action settings. Select the Action Type to FTP, then, the relevant settings at the bottom.

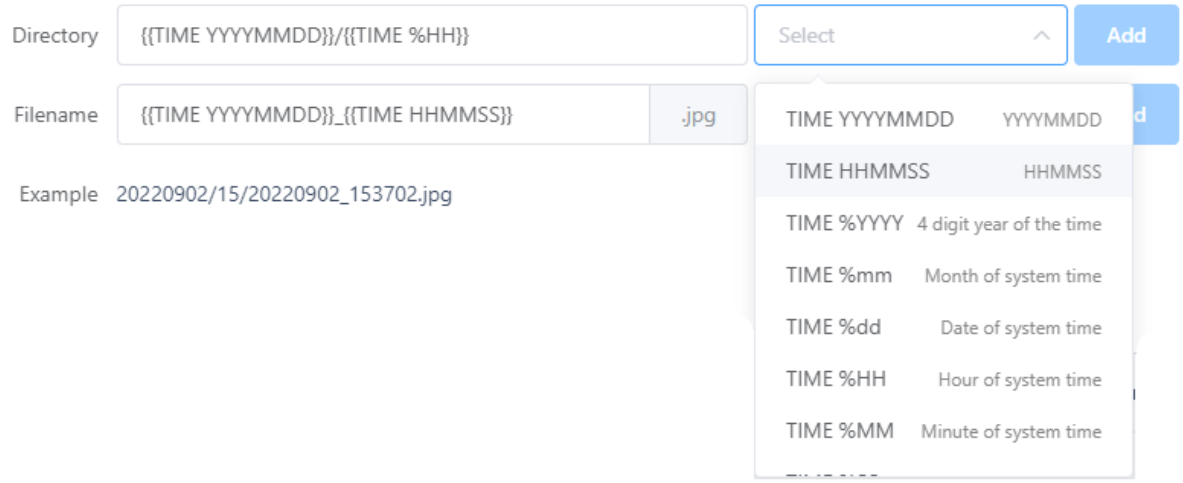
Snapshot Time Range Settings

1. Set the time range for uploading snapshots based on the time of the event.

In the example set above, snapshots taken from 2 seconds before the event to 1 second after the event will be uploaded.

Periodic snapshots are taken at least once per second for each channel, in addition to event snapshots.

Snapshot Upload Directory and File Name Format Settings



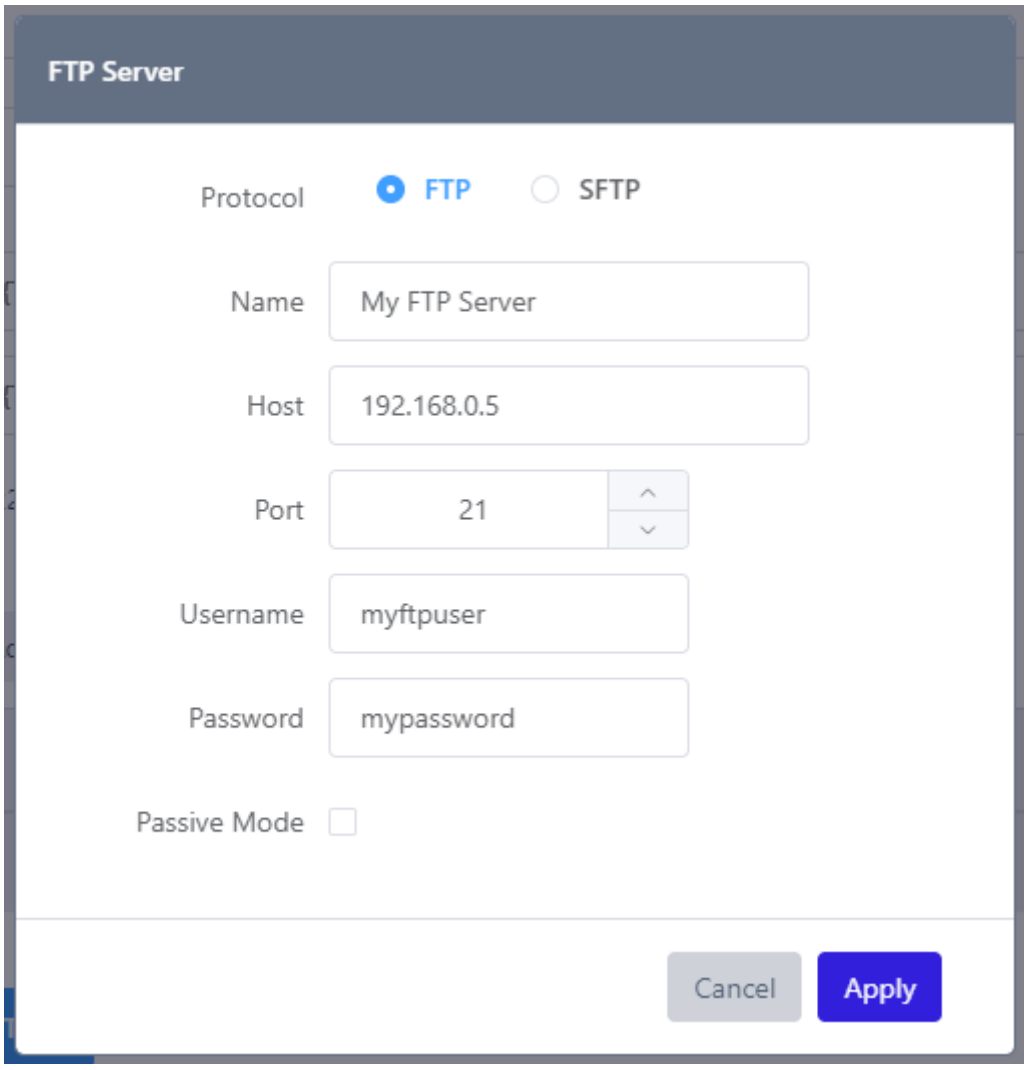
- **Directory** : Specify the location where the snapshot image is stored when the FTP Upload action is performed.
    - Event metadata can be included in this setting. Setting the path to include timestamps, as in the setting example above, specifies the upload directory based on the event time. The snapshot will be saved to the root directory of the FTP connection if this setting is not specified.
- **Filename** : Snapshot file names can be set similarly to directories.
    - The extension for snapshot file names is automatically set to .jpg, so there is no need to change it in the preferences.
- If you specify a snapshot file name, the Example shows an example path to the snapshot created by the directory and file name you specify.

FTP Server settings

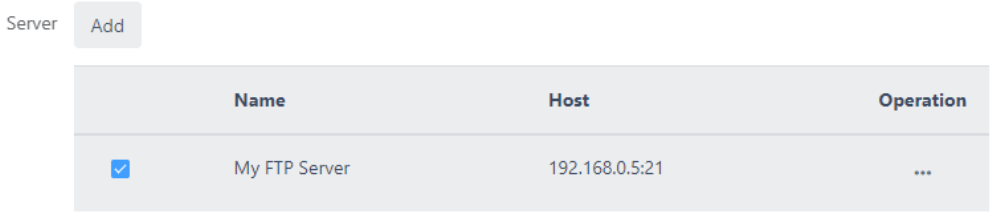
In the Server item, add the FTP server settings you want to transmit.

Once added, the FTP server settings can be used to set up other rules or FTP uploading actions in other applications.

1. Click the Add button to add new server settings.



2. Enter the destination FTP server information and click the Apply button.



After adding an FTP server setting, a new entry is added to the FTP server list.
Select the desired server in the FTP server list to complete setting up the server.

AWS S3 Upload

AWS S3 Upload action uploads event snapshots to AWS S3 storage when an application event occurs. The passkey value for the storage storing the snapshot file can be set using event metadata.

AWS S3 Upload Action can be added from the Action settings. Select the Action Type to **AWS S3**, then, the relevant settings at the bottom.

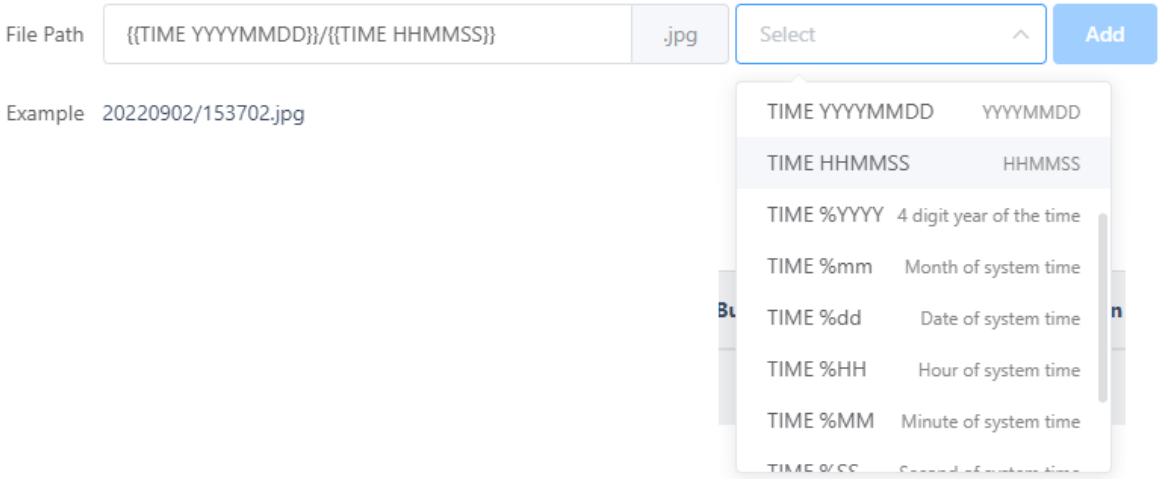
Snapshot Time Range Settings

1. Set the time range for uploading snapshots based on the time of the event.

In the example set above, snapshots taken from 2 seconds before the event to 1 second after the event will be uploaded.

Periodic snapshots are taken at least once per second for each channel, in addition to event snapshots.

Snapshot Upload File Path Settings



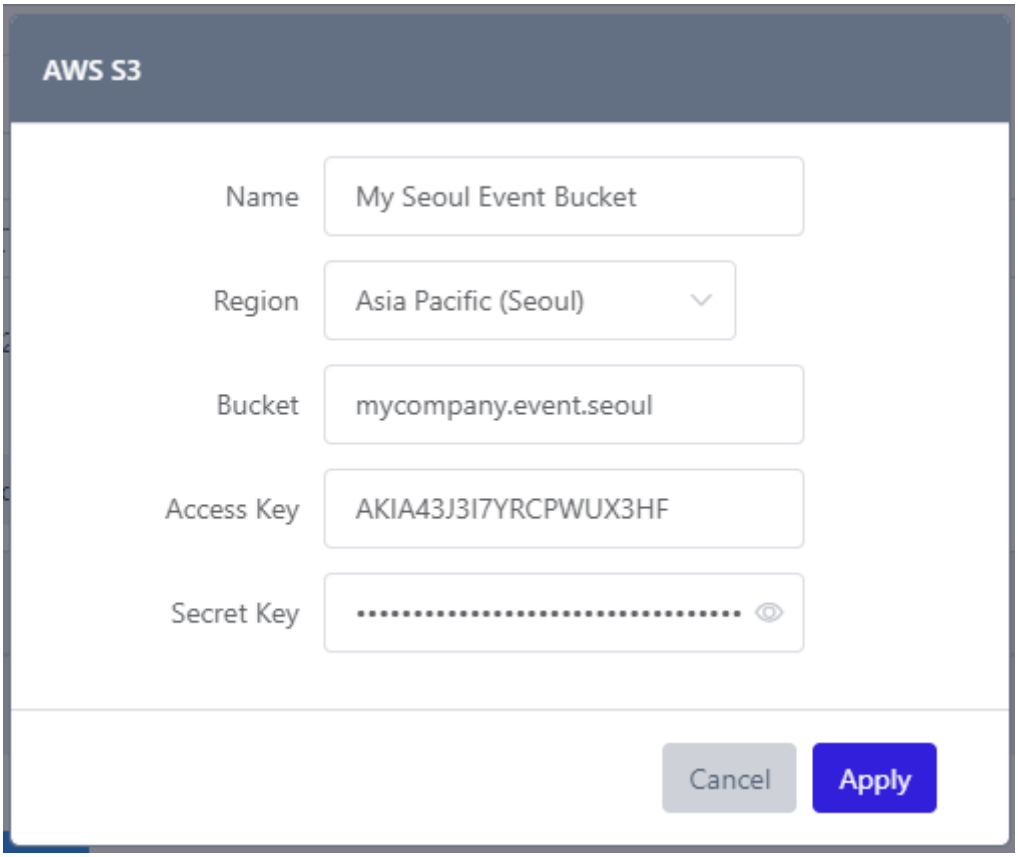
- **File Path** : Specify the path where the snapshot is stored.
    - Event metadata can be included in this setting. Setting the path to include time metadata, as in the example above, sets the upload file path based on the time the event occurred.
    - Set a file path excluding the Region and Bucket parts. You only need to set the path within the bucket where the file will be saved.
- After setting the file path, the Example section shows an example snapshot path.

AWS S3 Storage Settings

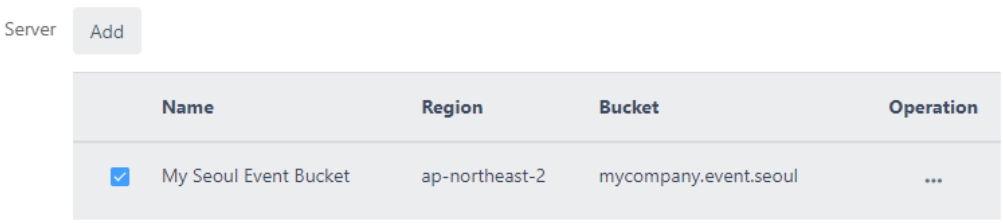
Add AWS S3 storage settings to the Server item.

Once added, AWS S3 storage settings can be used to set other rules or to set AWS S3 upload actions in other applications.

1. Click the Add button to add new server settings.



2. Enter your target AWS S3 store information.
3. Click the Apply button to save the settings.
4. Once your AWS S3 storage has been added, it will be listed.

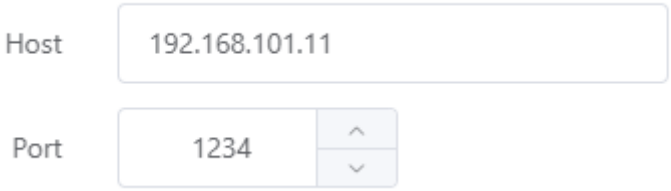


   - Once you have ticked the destination box, the setup process for your AWS S3 storage is complete.

TCP Communication

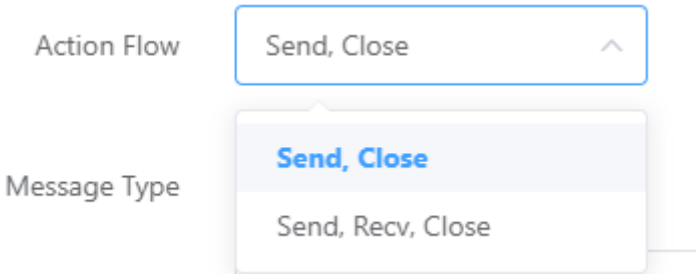
You can connect to a TCP server and transmit data when an application event occurs.

Server configuration



You can set the server's IP address and port number.

Action Flow



Send, Close

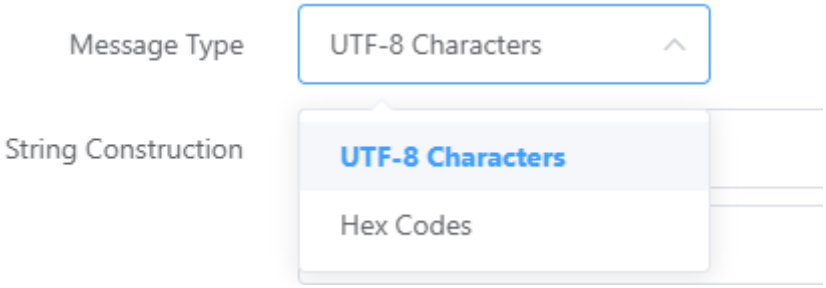
After connecting to the server, send the preconfigured message and then terminate the connection.

Send, Recv, Close

After connecting to the server, send the preconfigured message and receive the response message before terminating the connection.

The response timeout is 3 seconds.

Message Type



You can set the message type to two options.

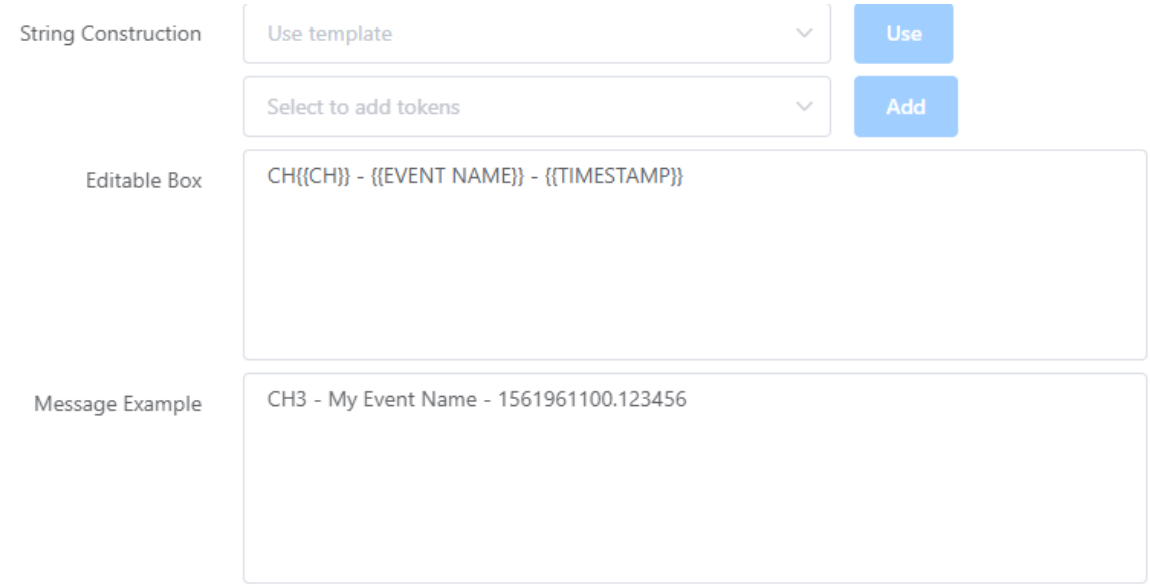
The UTF-8 type is used for standard text messages with UTF-8 encoding.

Hex Codes represent binary data values in hexadecimal format.

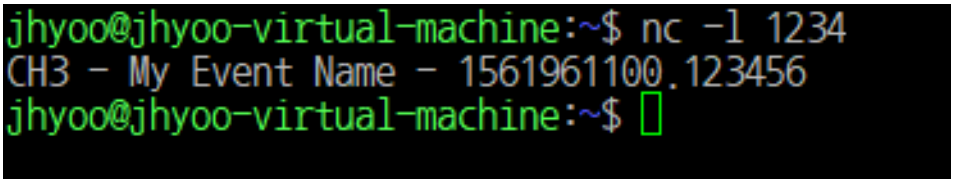
UTF-8

The UTF-8 format can be configured using tokens and templates. Please refer to the configuration examples.

Configuration examples



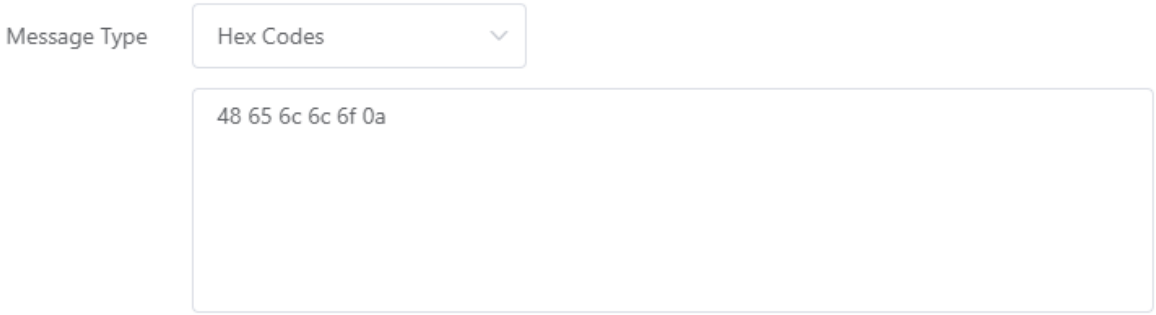
Reception examples



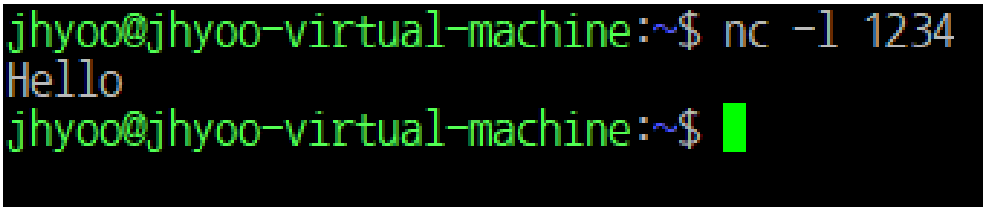
Hex Codes

In the Hex Codes format, tokens cannot be used; however, you can configure raw data using hexadecimal values. Please refer to the configuration examples.

Configuration examples

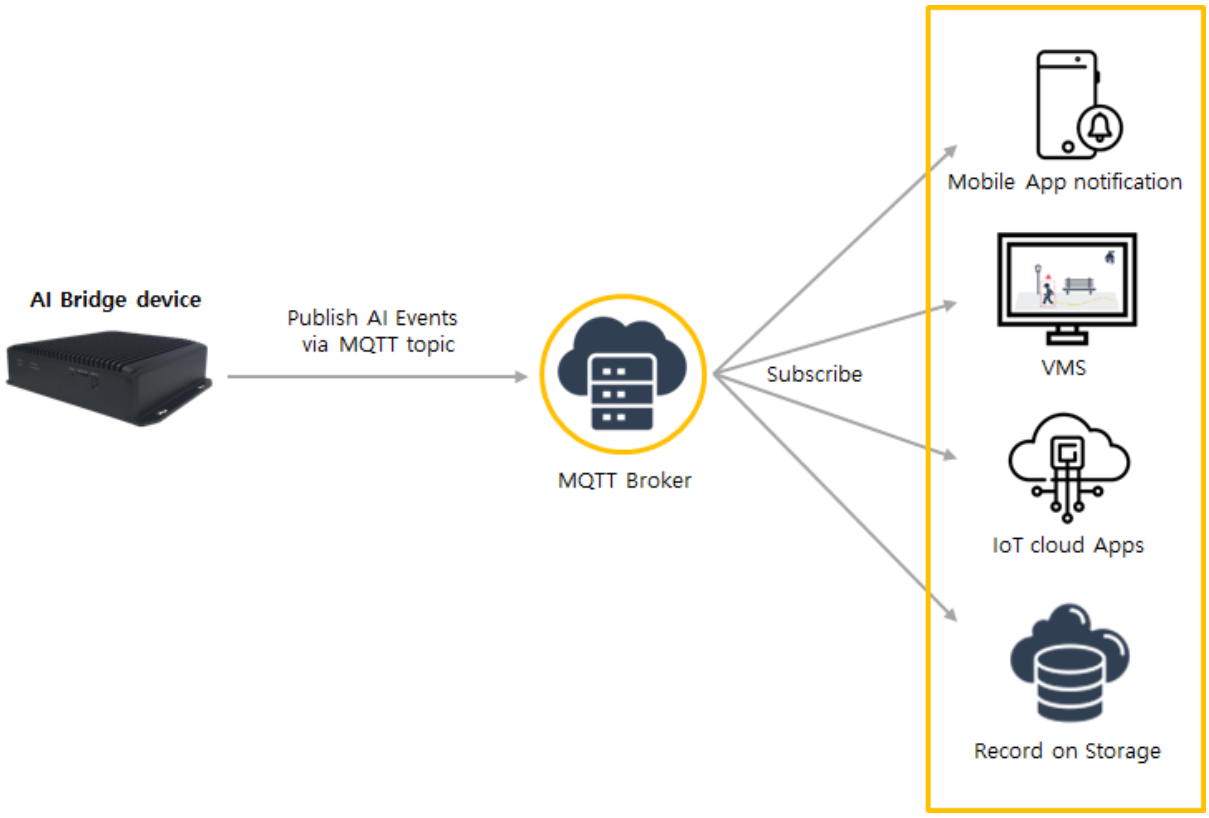


Reception examples



MQTT Publish

You can use the publish feature of MQTT to integrate AIBOX with a variety of devices.



1. MQTT?

MOTT(Message Queuing Telemetry Transport) is a lightweight messaging protocol that is ideal for efficient communication in low-bandwidth or unreliable network environments, particularly with IoT(Internet of Things) devices. Its lightweight nature makes it specifically designed for delivering messages between remotely connected devices.

MQTT Features

- Lightweight protocol :MQTT is an efficient protocol for low-bandwidth and resource-constrained environments.
- Asynchronous communication : Clients able to send first and receive messages at a later time.
- Quality of Service(QoS) Level: MQTT also offers various Quality of Service (QoS) levels to guarantee message delivery reliability.
- Last Will and Testament(LWT) messages: The messages is sent when a client experiences an unexpected disconnection.

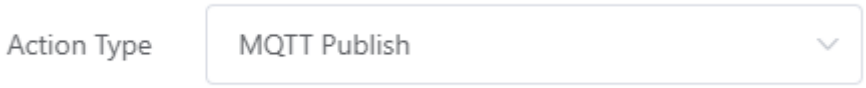
Main components of MQTT

- Broker
    - The MQTT broker is server as a relay between clients, transmitting messages.
    - The broker receives messages from clients and forwards them to other clients subscribed to the topic.

- The broker typically functions as a centralized server, serving as the hub for all message exchange.

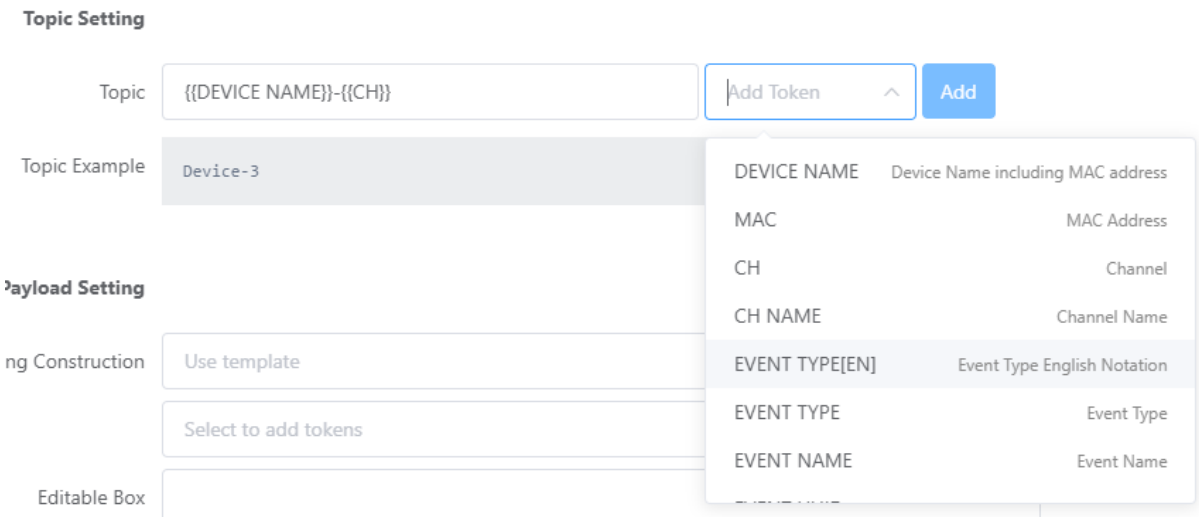
- Client
  - MQTT clients are endpoints that send and receive messages.
  - Clients can publish messages to the broker or subscribe to specific topics.
  - Clients can take many forms, including IoT devices, mobile apps, and server applications.
- Topic
  - Topics in MQTT define how messages are categorized.
  - Topics are strings that can be hierarchical. (Ex: “home/livingroom/temperature”)
  - Clients subscribe to the topics they are interested in, and receive messages only about those topics.
- Message Payload
  - The message payload is the data component of the MQTT message.
  - It can vary in form, including text or binary data, and its size is determined by the broker’s implementation.
  - The message payload contains the information that the client wants to send to other clients.

2. How to set up the MQTT Publish action



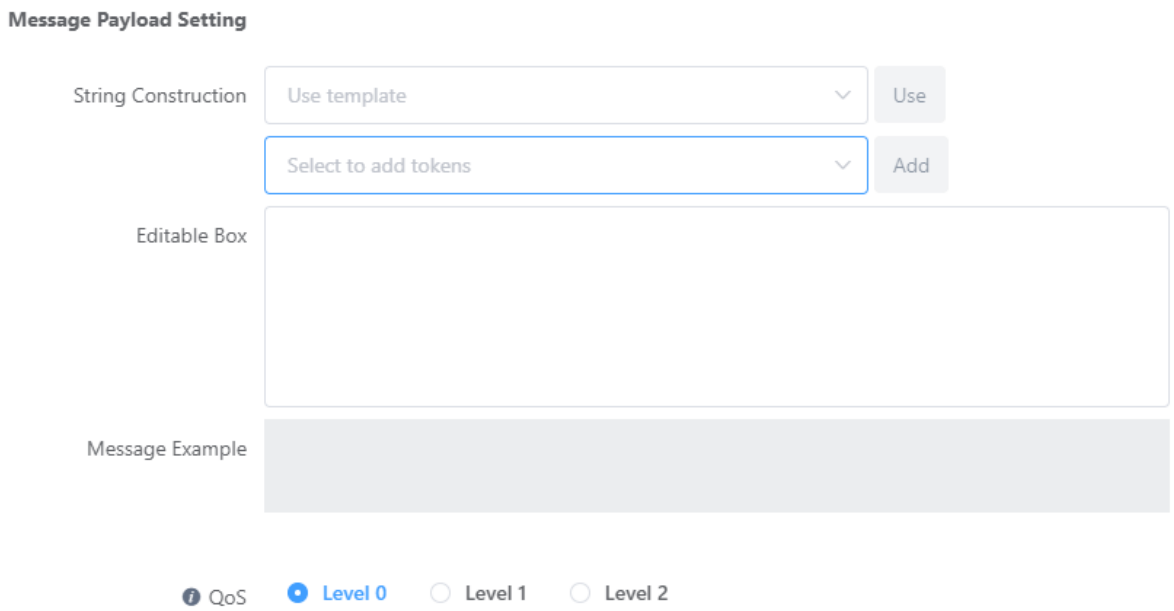
Select **“MQTT Publish”** as the **action type** and click “Add” to show the relevant settings.

– Topic Setting



Set the Topic. You can input which can be a specific phrase or a predefined token.

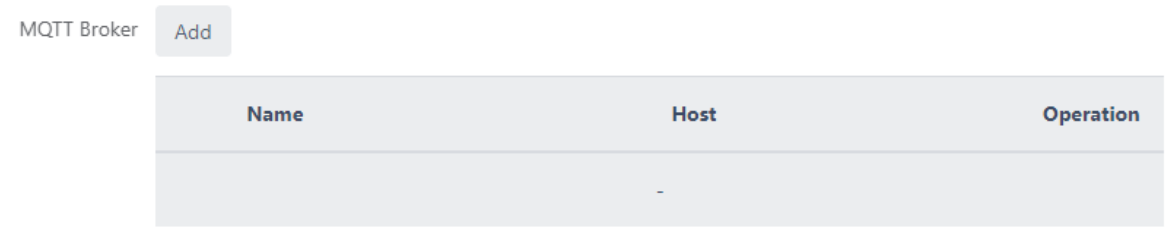
– Message Payload Setting



You can set the Message Payload and set the QoS level.

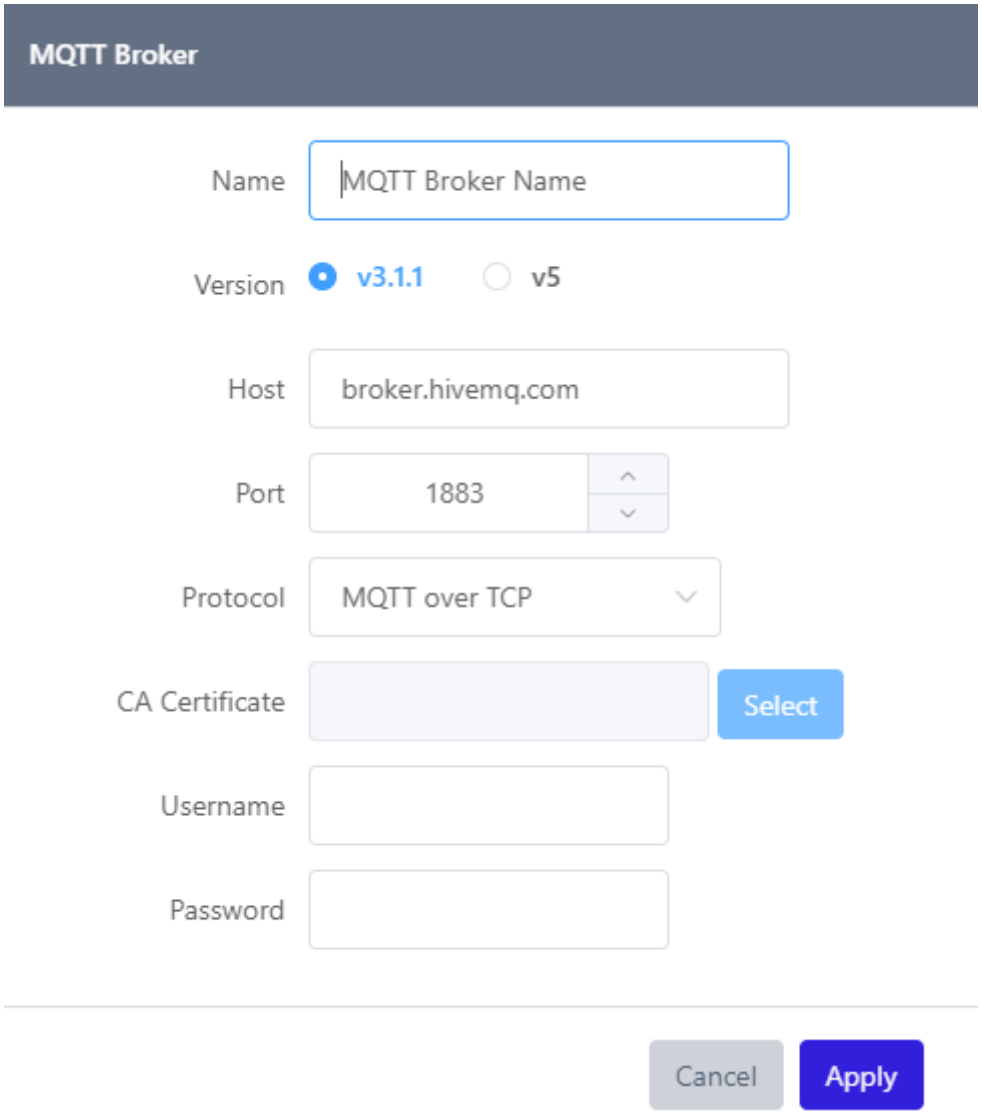
Please refer to “Utilizing Event Meta Tokens & Creating Action Message Guide” for how to set the Message Payload.

– MQTT Broker Setting



You can add an MQTT Broker, or select a Broker to use from the added MQTT Brokers.

Click the ‘Add’ button to display a menu to add an MQTT Broker.



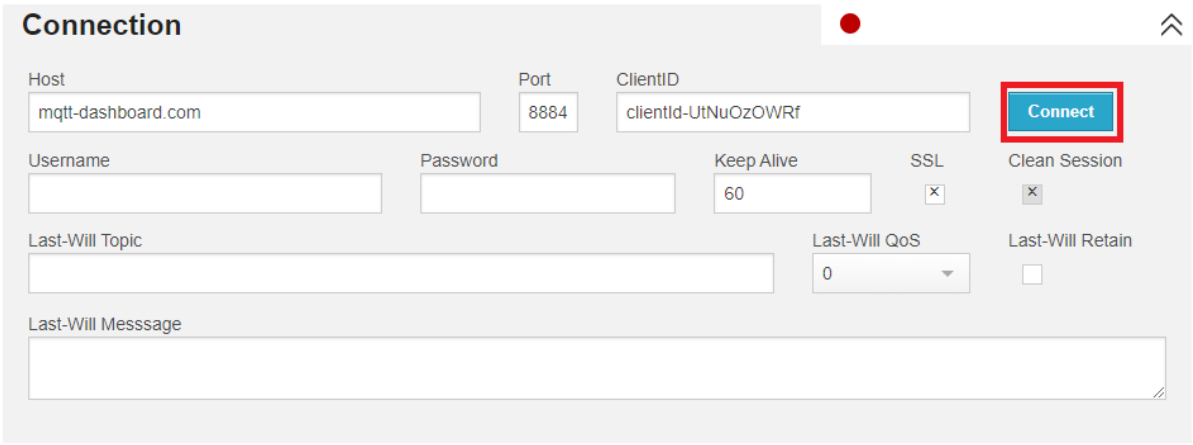
You can set the name of the MQTT Broker and set the MQTT Broker access information.
If you need help with access information, contact your MQTT Broker representative.

3. How to test the MQTT Publish action

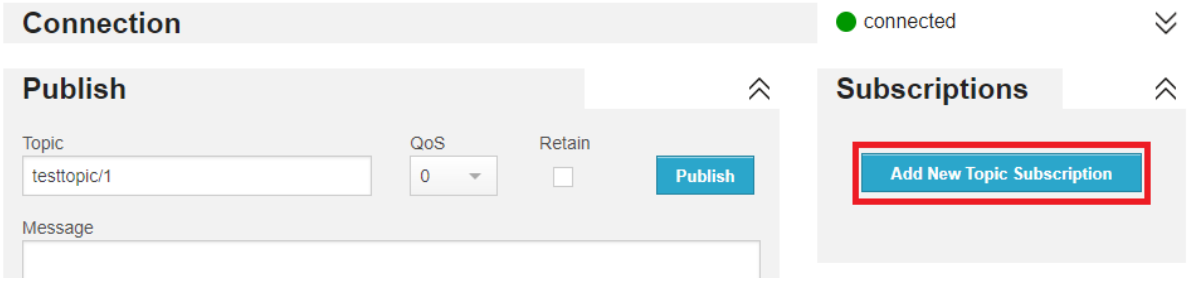
Here show you how to test using the MQTT Broker and MQTT Web Client, both of which are available for free from hivemq.

– MQTT Client : Subscribe Setting

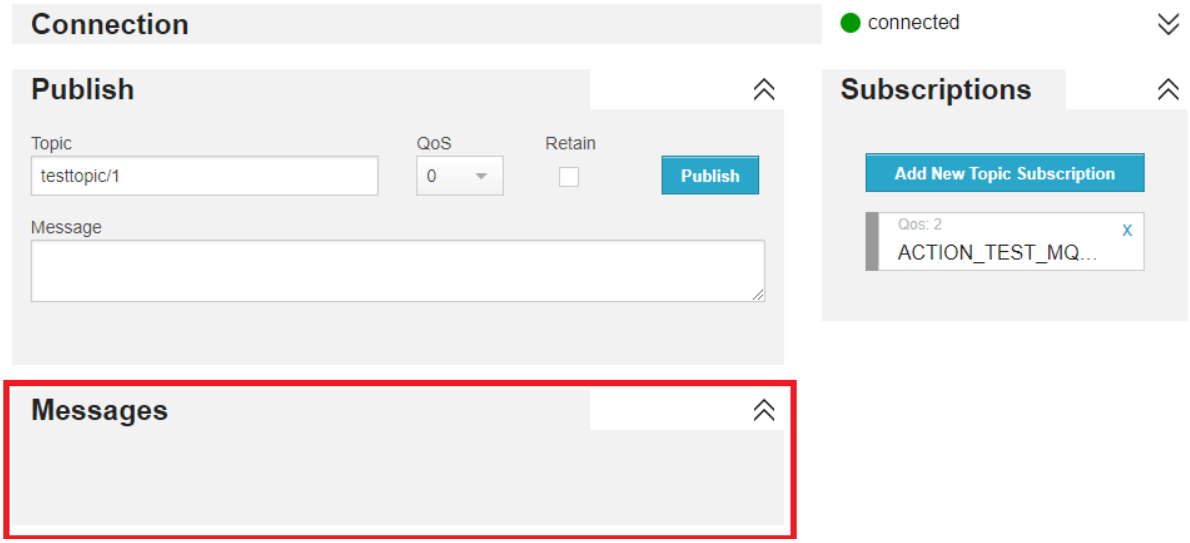
Access to hivemq's MQTT Web Client. Click the Connect button, as the connection to the hivemq free broker is already established by default.



Click the “Add New Topic Subscription” button after connecting, and then input the name of the Topic (“ACTION_TEST_MQTT_PUBLISH”) you wish to configure in the MQTT Publish action.

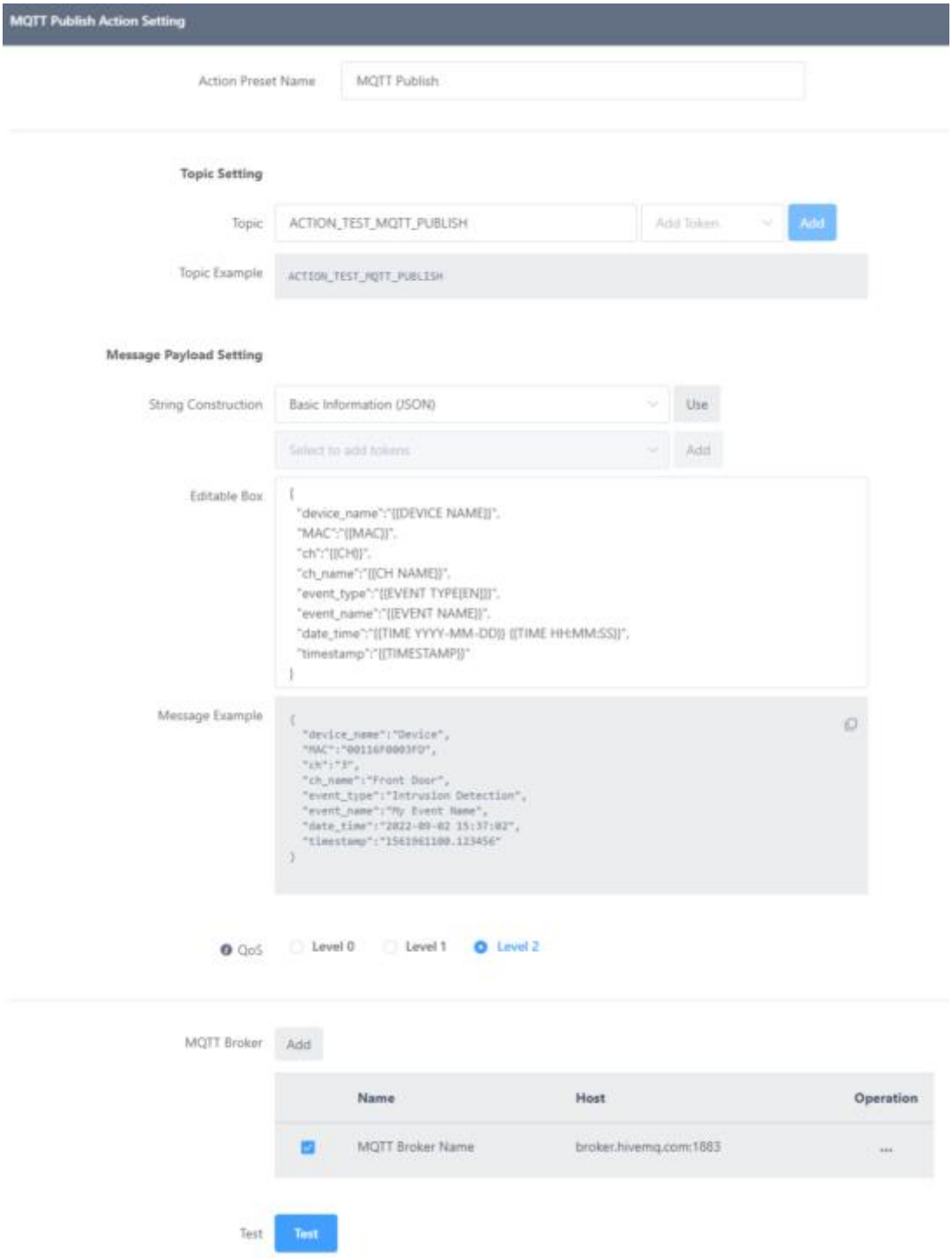


Once set up, you will see a page below. Check the Message section of this page for the test result once you have set up the MQTT Publish action.

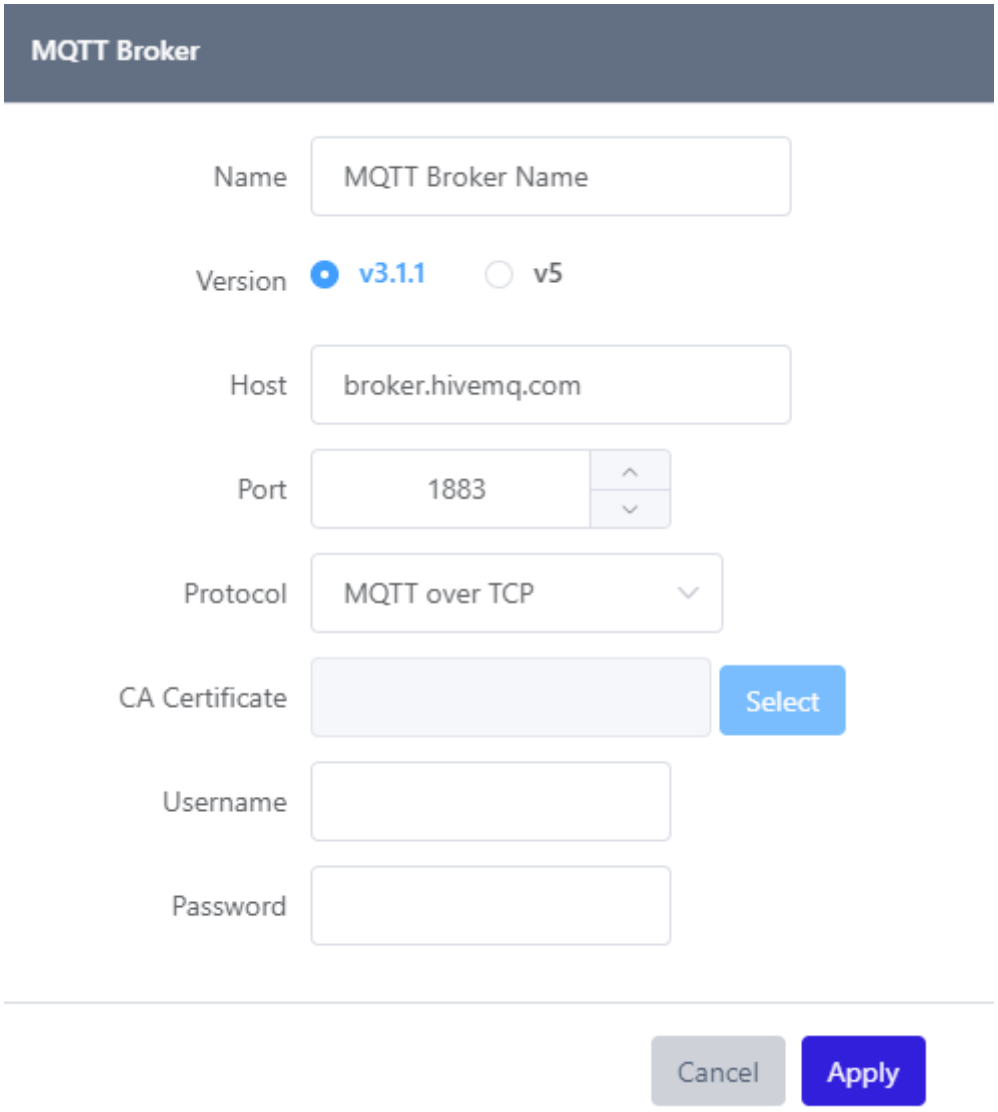


– MQTT Publish Action Setting

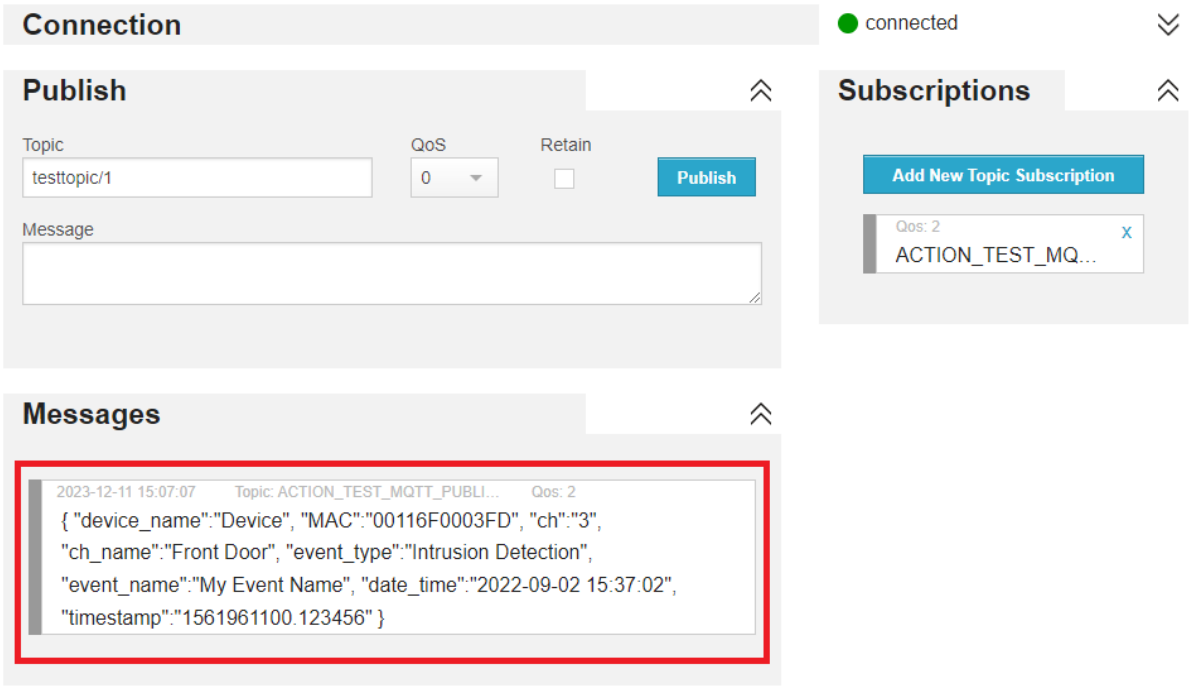
Set up the MQTT Publish action as follows.



Set up the MQTT Broker as follows.



After configuration, click the Test button to run the MQTT Publish Test Action. When you see the MQTT Web Client, the test result is displayed as shown below.



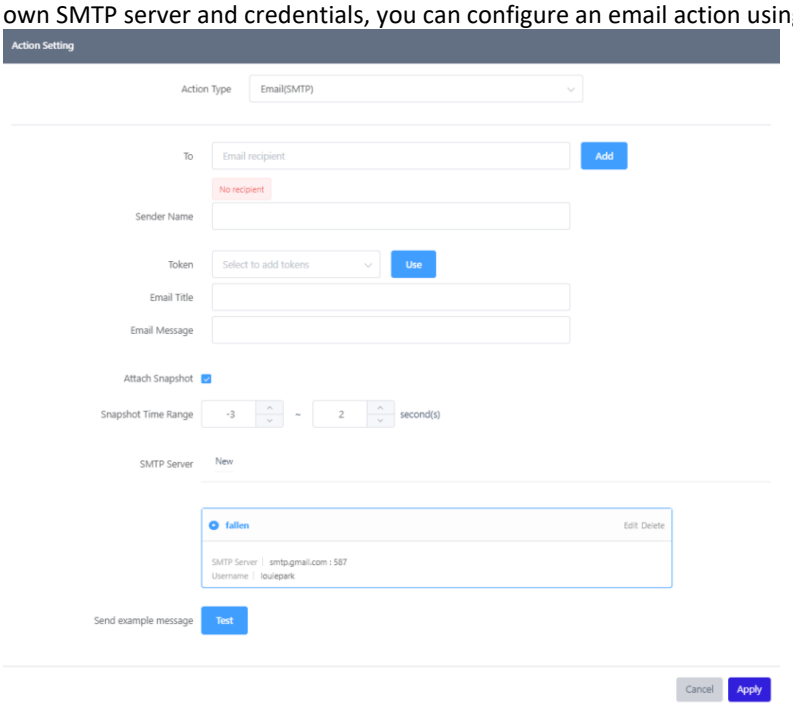
Email Alarm

You can email event snapshots and event metadata information when an event occurs.

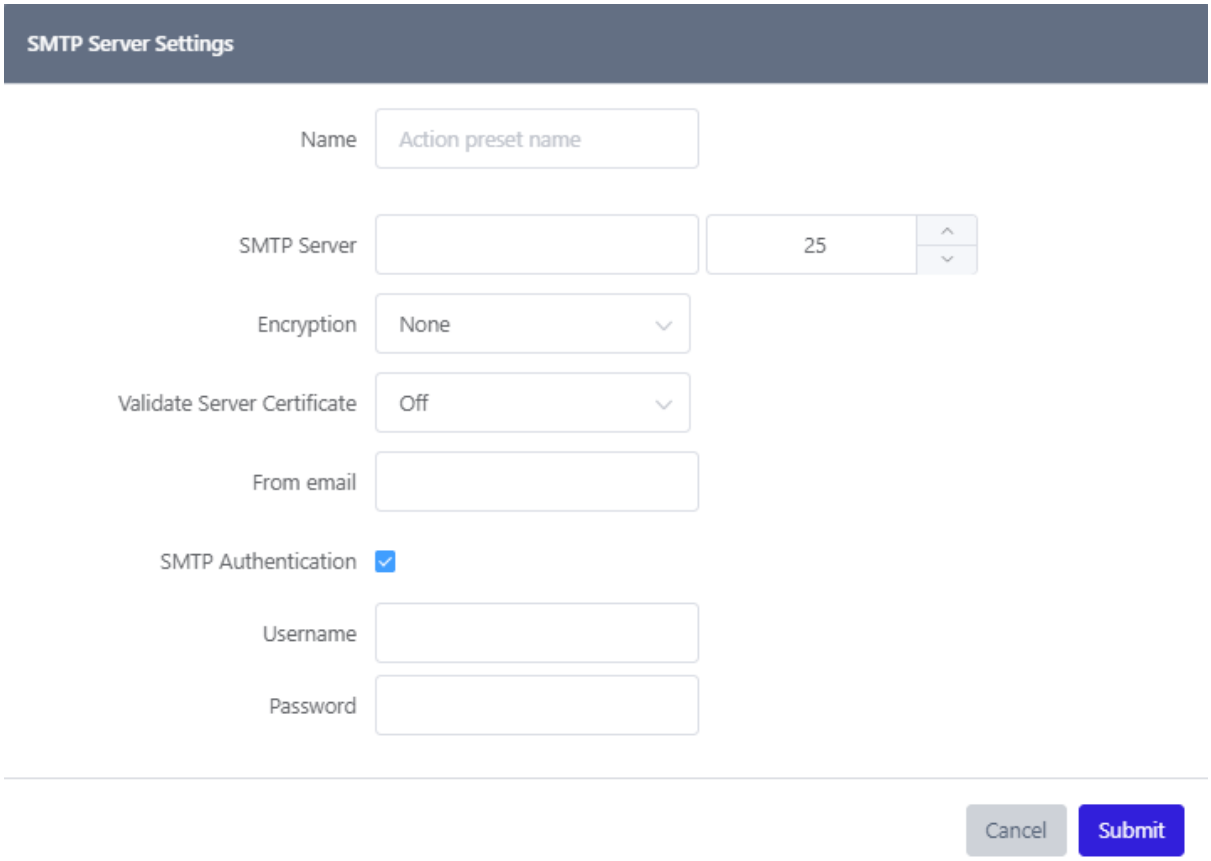
Email Action using an SMTP Server Settings

Email actions using an SMTP server can be added from the Action settings

1. Select the Action Type to Email(SMTP), then, the relevant settings at the bottom. If you set up your own SMTP server and credentials, you can configure an email action using that SMTP server.

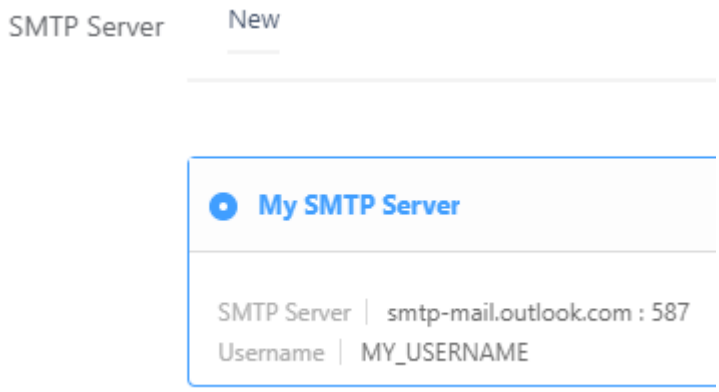


2. Click the New tap to add a new SMTP server configuration. Registered SMTP server configuration can be referenced to all event actions.



- **Name** : Enter a SMTP name.
- **SMTP Server** : Enter the address and SMTP server port.
- **Encryption**: Select the encryption method used by the server, such as SSL/TLS.
- **Validate Server Certificate** : If you set the Validate server certificate item to ON, the server includes a procedure to verify the certificate presented by the server with a certificate authority. If you use a certificate that a certificate authority has not verified, the email will not be sent.
- **From email** : Enter the sender's email address if required by the SMTP server.
- **SMTP Authentication**: Enter the SMTP server authentication information.

3. If an SMTP server is added, it shows in the SMTP server list. Select one to configure the email alarm action.



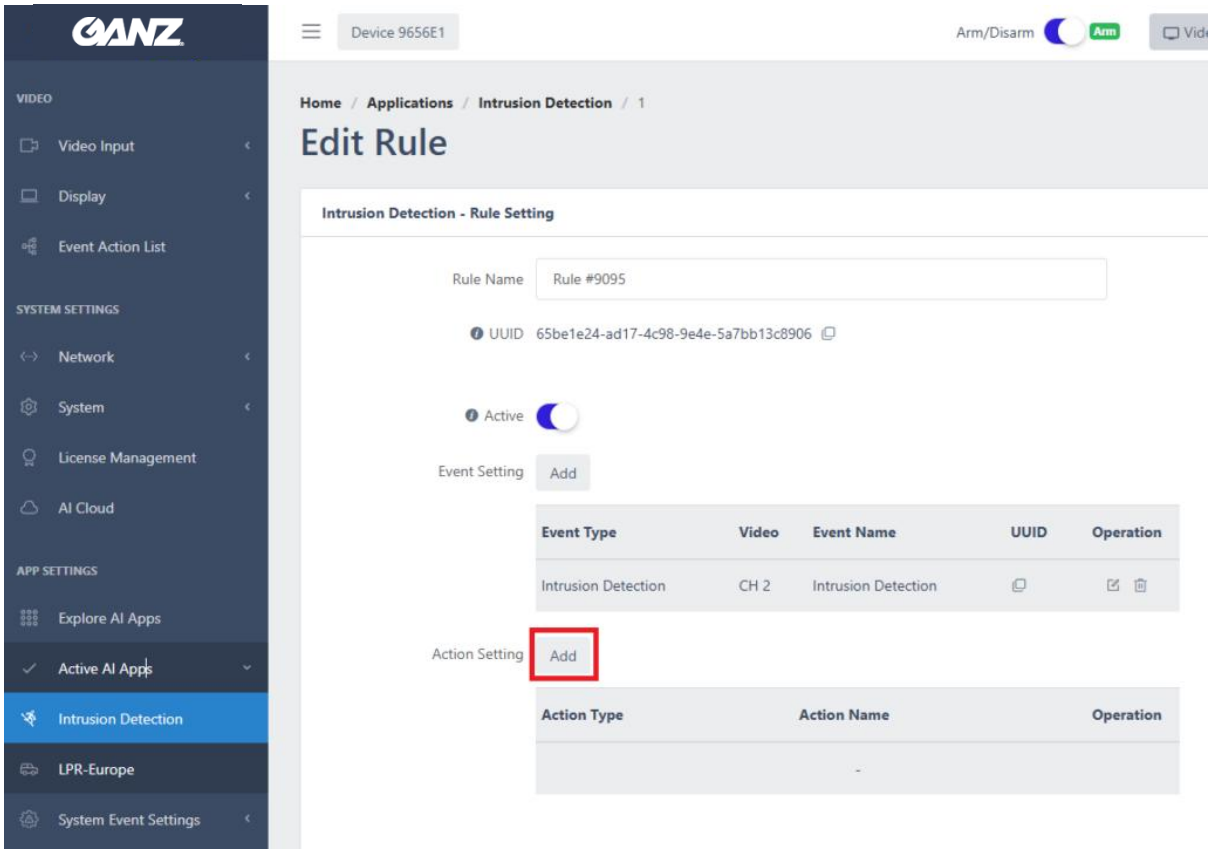
Video Clip / Snapshot

Video Clips and Snapshots can be attached to AI App Actions such as: Email, HTTP, FTP and AWS. The video clip consists of 3 to 5 clips, and the snapshots last about 2 to 3 seconds.

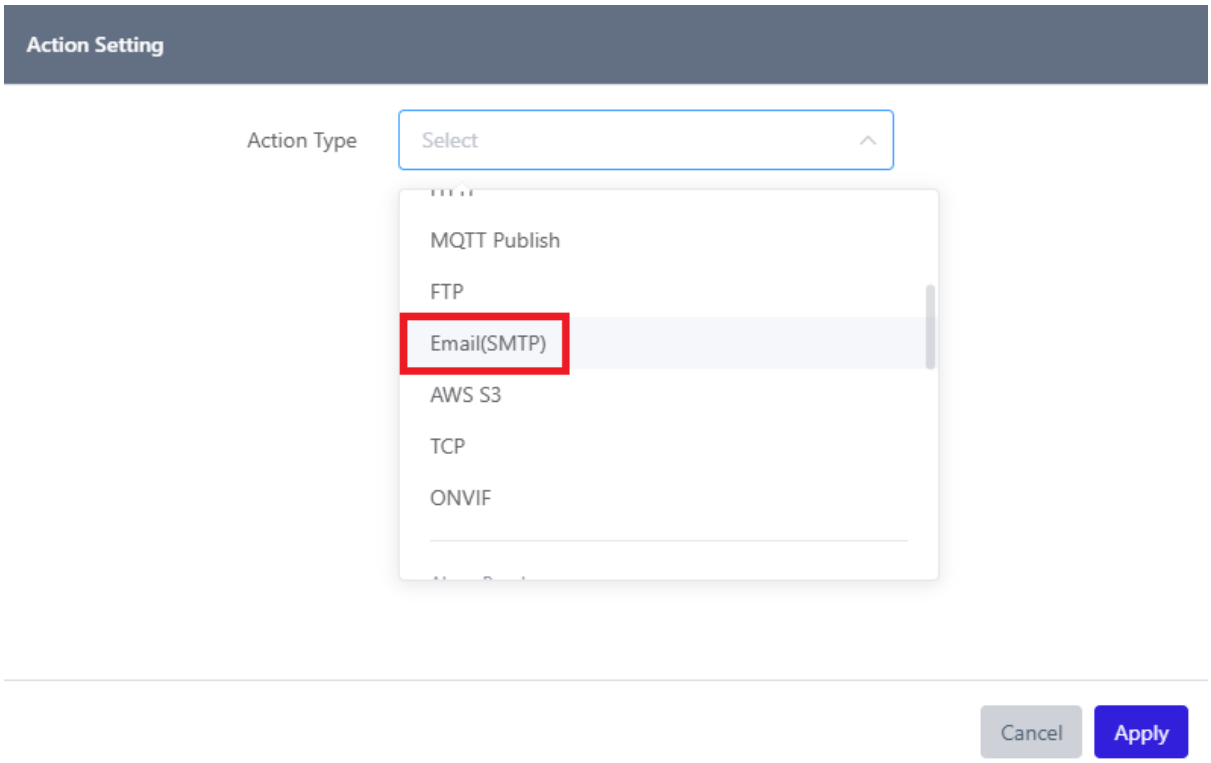
Note. The Video Clips and Snapshots will be .TS files, in most cases you will need to install VLC player to view them.

Follow the steps below to add Video Clips and Snapshots to an Action.

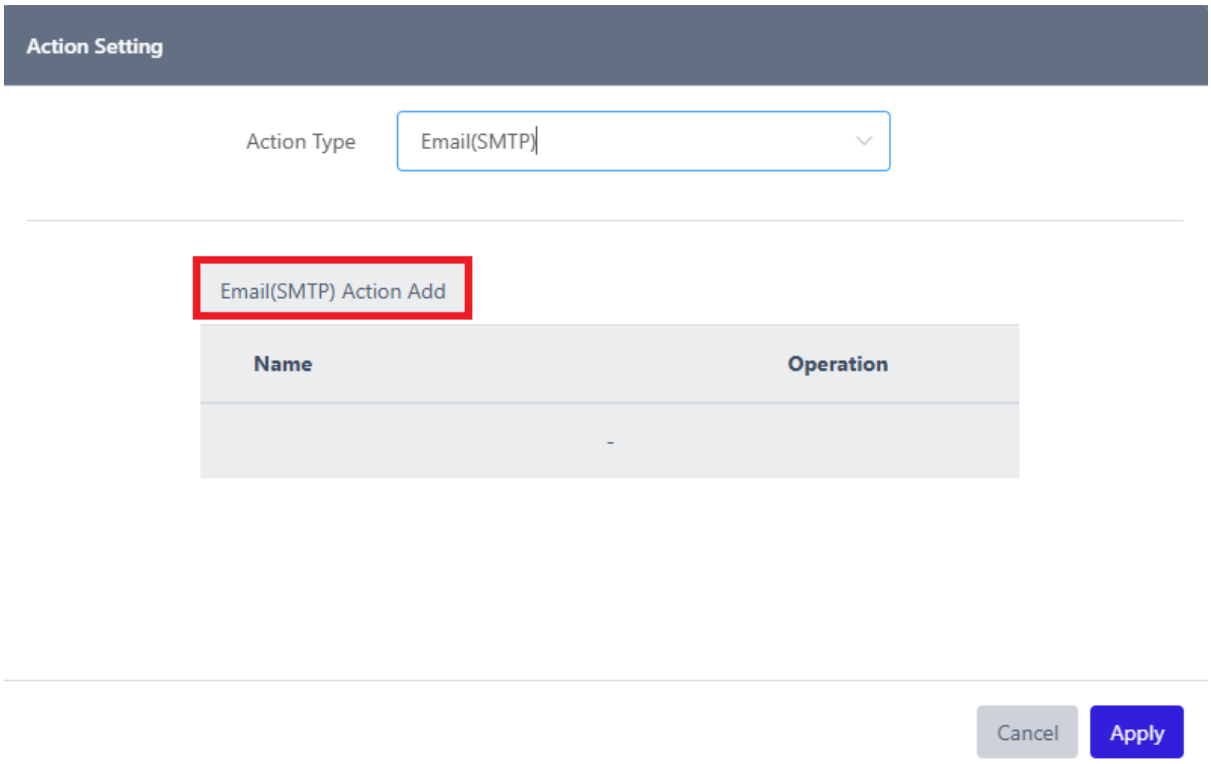
In this example, we will navigate to **Applications > Intrusion Detection**, then click on the **Add** button.



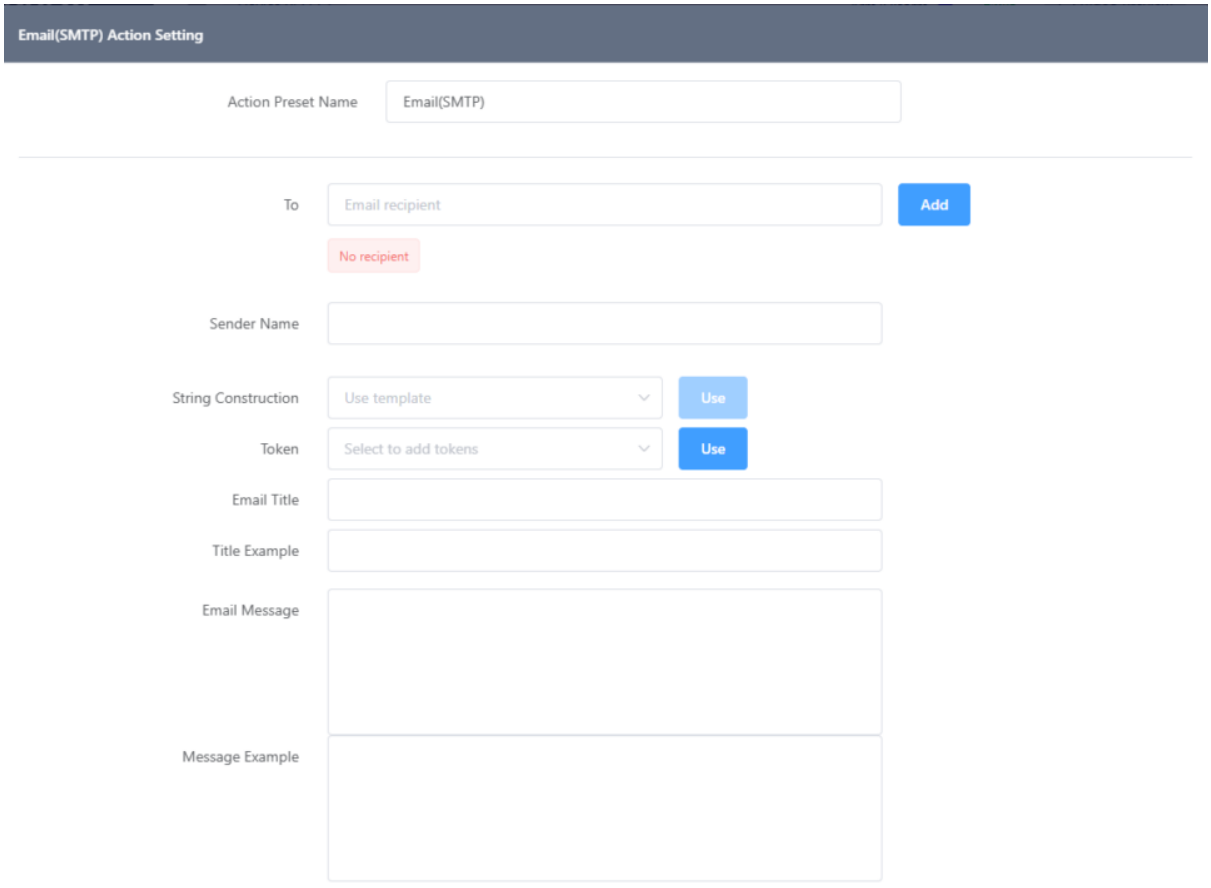
Select **Email(SMTP)** from the Action Type drop-down list.



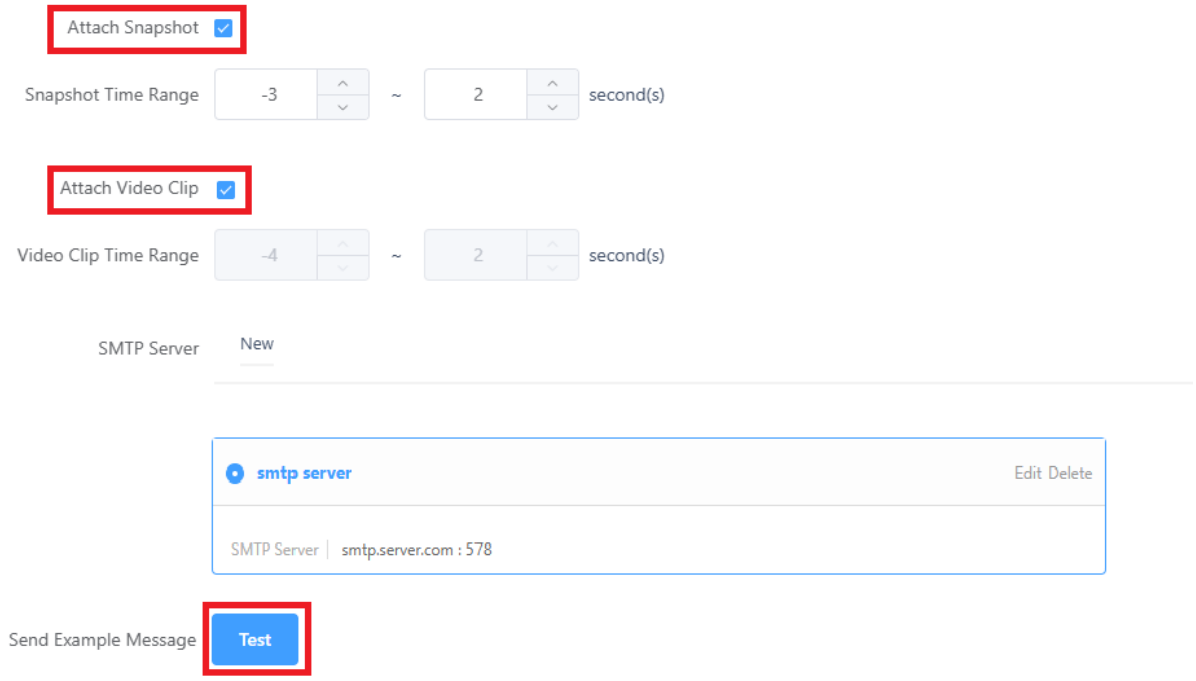
Click on the **Email(SMTP) Action Add** Button.



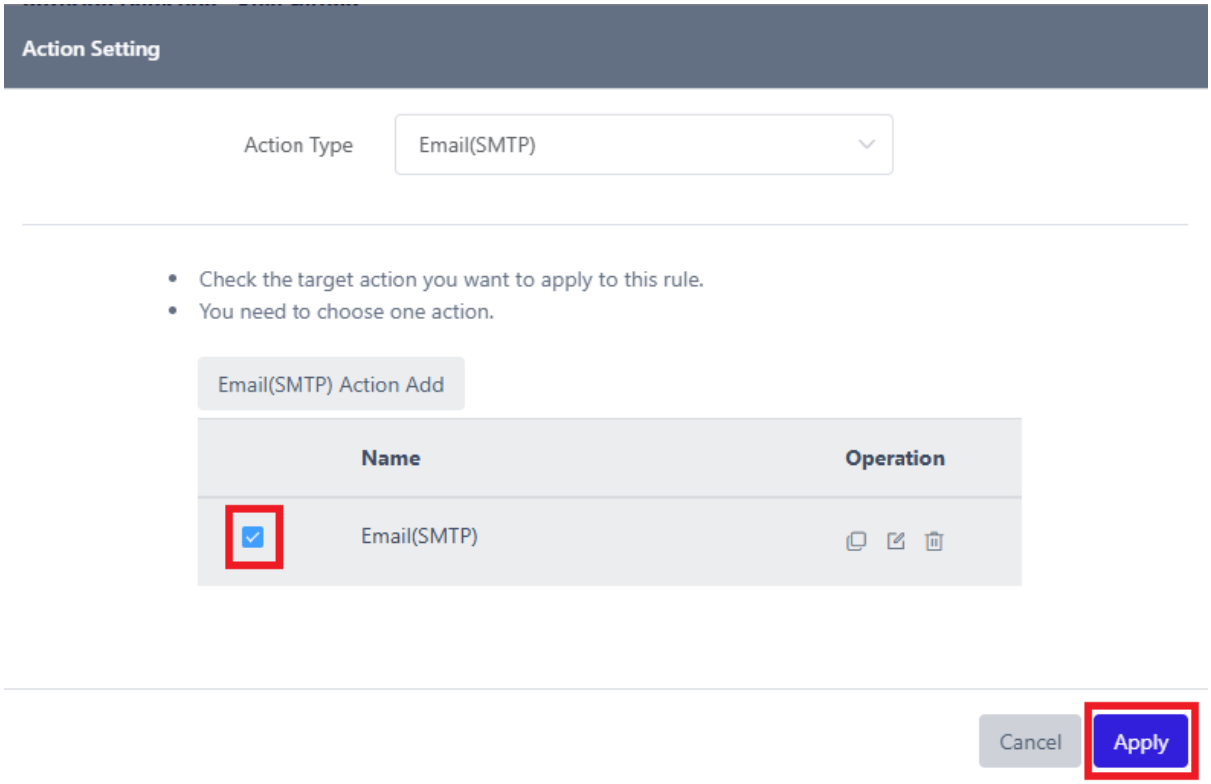
Add an email that you have previously configured



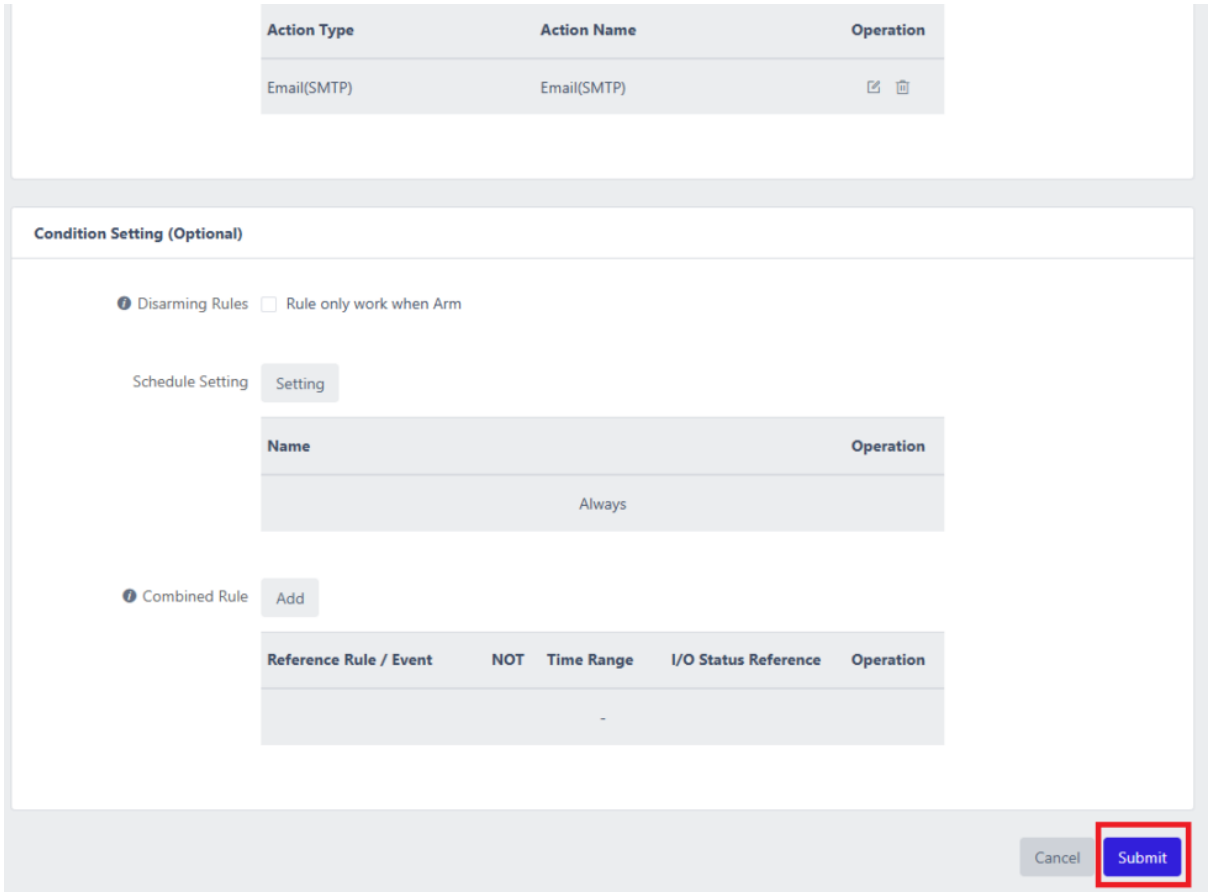
Scroll down the page and enter an optional email message, then select the **Attach Snapshot** and **Attach Video Clip** option. Next, click on the **Test** button to test the email settings. When done, click on the **Apply** button to close the window.



Click **Apply** again on the next window.



Finally select **Submit** to save your changes.



You should now receive snapshots and video clips to the email address you have set up when an event occurs.

VMS / Alarm Monitoring

Avigilon ACC Integration Guide

1. Introduction

1.1 Prerequisites

- AIBOX FW version 103000 or greater.
- Avigilon ACC 7.14 or greater.

1.2 Learn about integration architecture

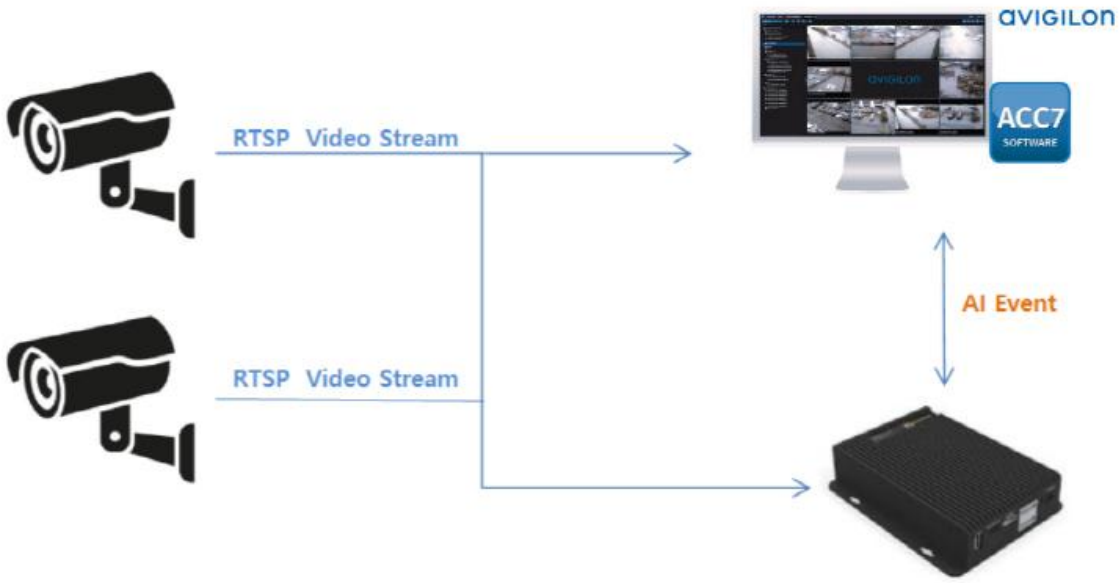
There are two ways to integrate AIBOX with Avigilon ACC VMS:

1) Case 1

The AIBOX receives the RTSP video stream from the IPCAM and provides the annotated video and event data after AI analysis. The annotated video is transcoded to provide object recognition information, bounding boxes, zone information, and more from AIBOX's AI analysis.

2) Case 2

Both AIBOX and Avigilon ACC VMS simultaneously receive the RTSP video stream from the IPCAM, and the AIBOX sends the AI analysis events to Avigilon ACC VMS. It can also receive the RTSP stream from Avigilon ACC VMS instead of the IPCAM's RTSP video stream.



2. Configuration

2.1 Avigilon ACC VMS Configuration

We will explain how to integrate AIBOX with Avigilon ACC VMS using the Case1 method.

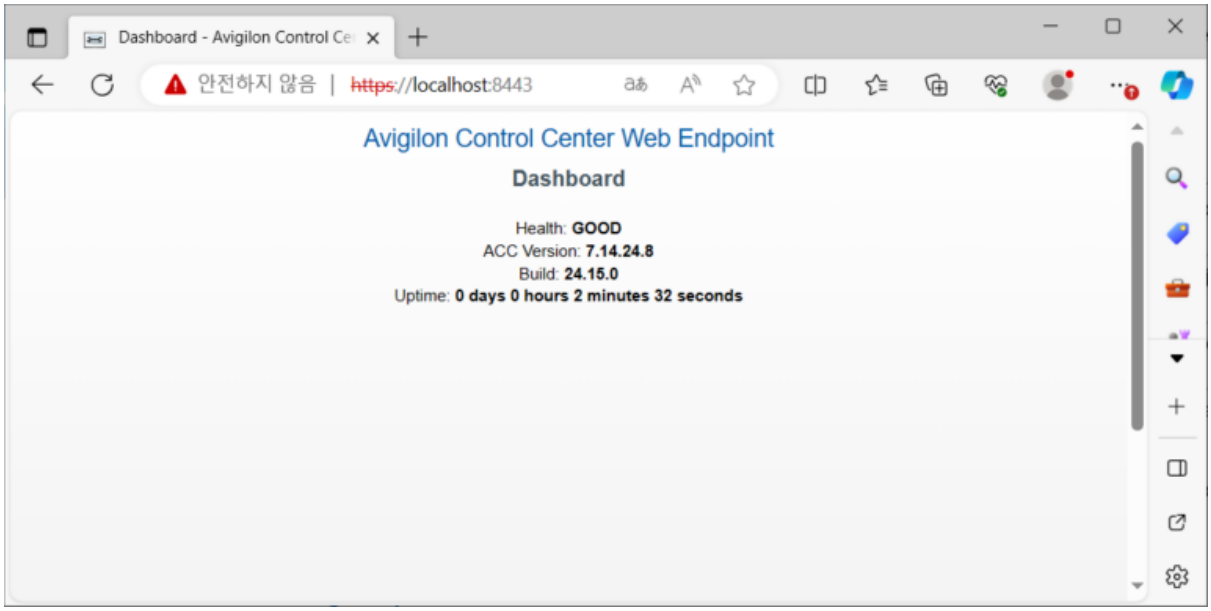
1) Installing the ACC Web Endpoint Service

The ACC Web Endpoint Service must be installed on the same system as the ACC Server software.

Download and install the ACC 7 Web Endpoint Service from the Avigilon website:

https://www.avigilon.com/software-downloads

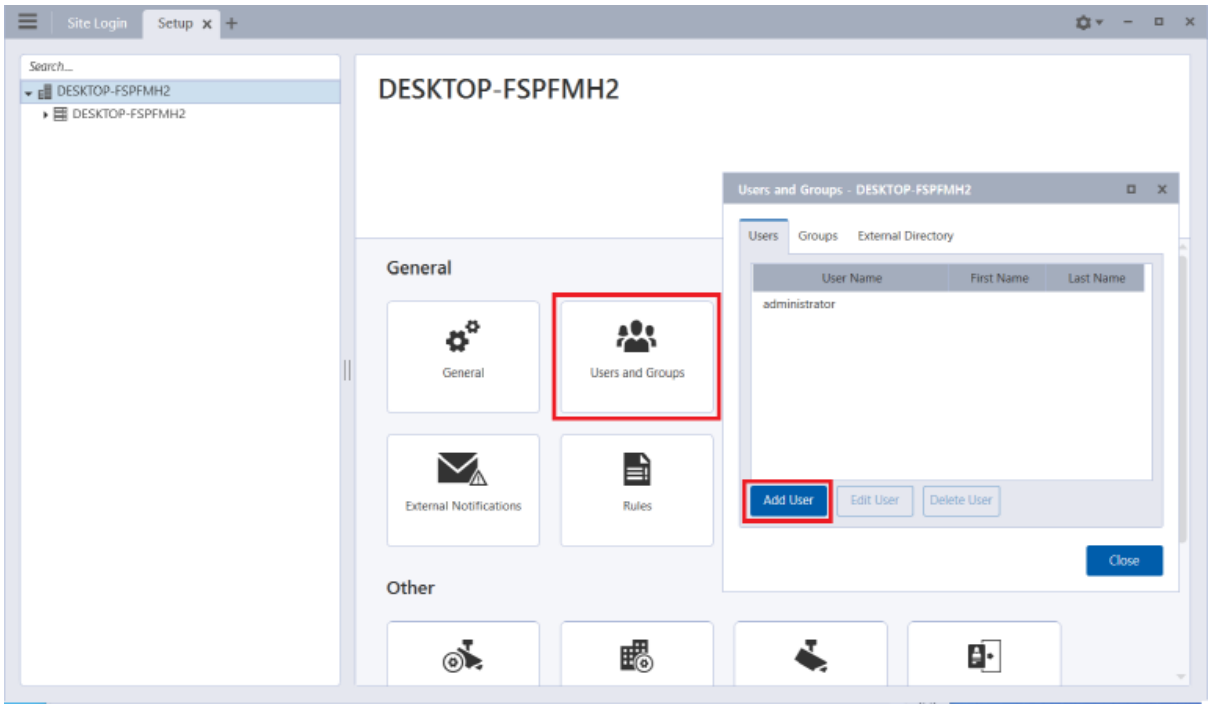
Once installed, you can view the health of the ACC 7 Web Endpoint Service at: https://localhost:8443/



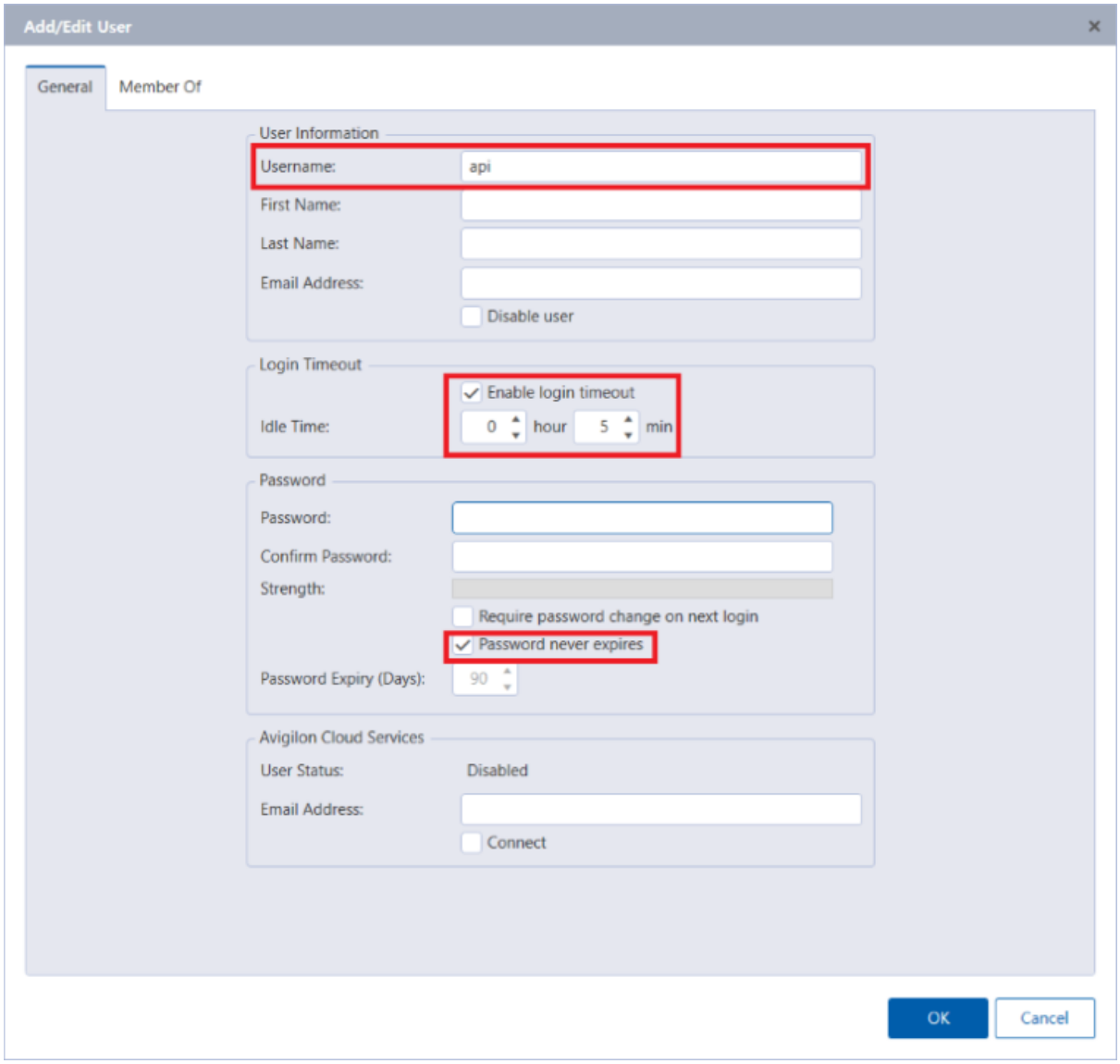
2) To add an ‘api’ account to Avigilon ACC VMS

To integrate AIBOX with Avigilon ACC, you add an account that will be used for the integration. In this document, we will create an ‘api’ account.

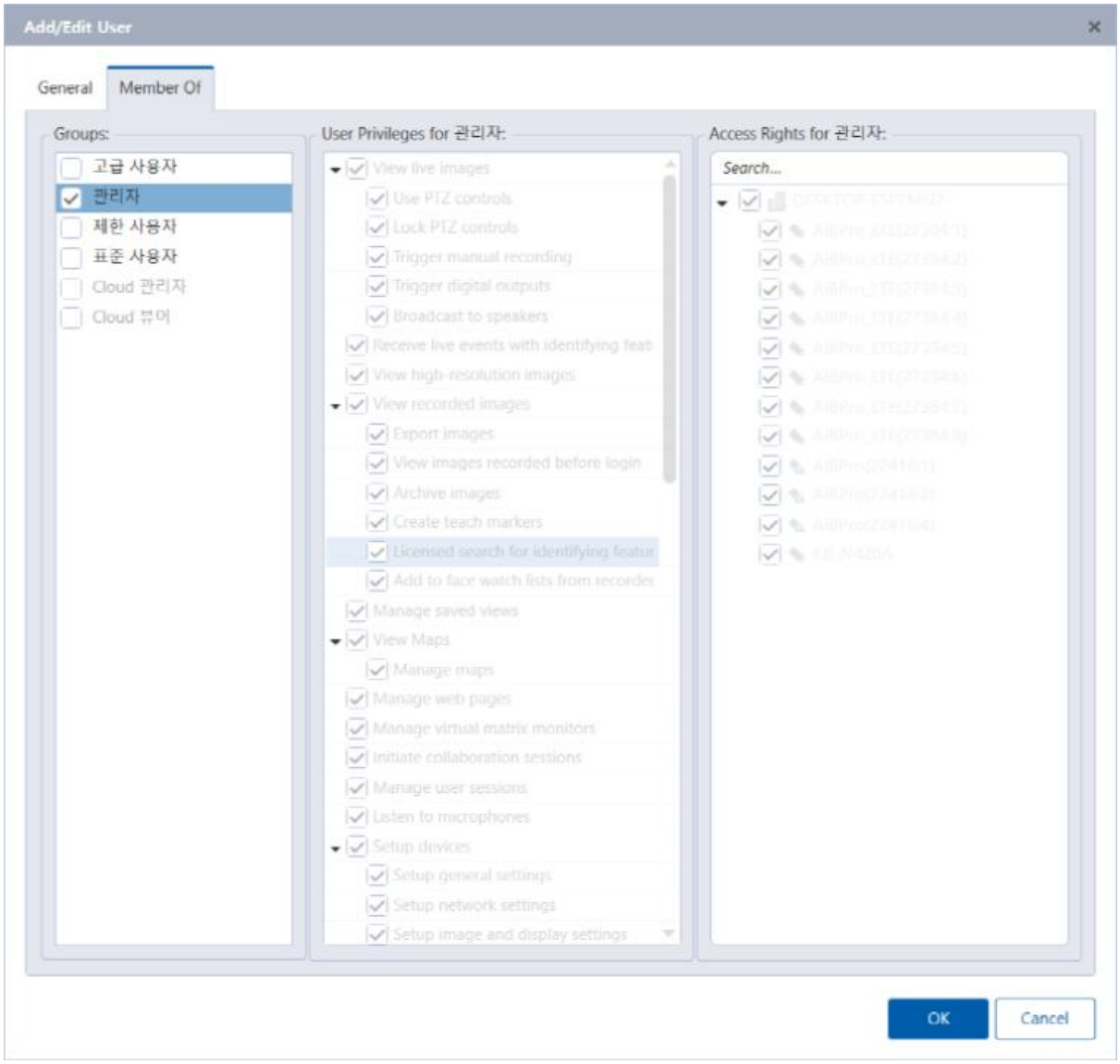
Click on ‘Users and Groups’ in the site settings of the Avigilon ACC Client, then click on ‘Add User’.



Enter the Username as ‘api’ and set the Login Timeout to 5 minutes. Then, make sure to set the password so that it does not expire (check ‘Password never expires’).

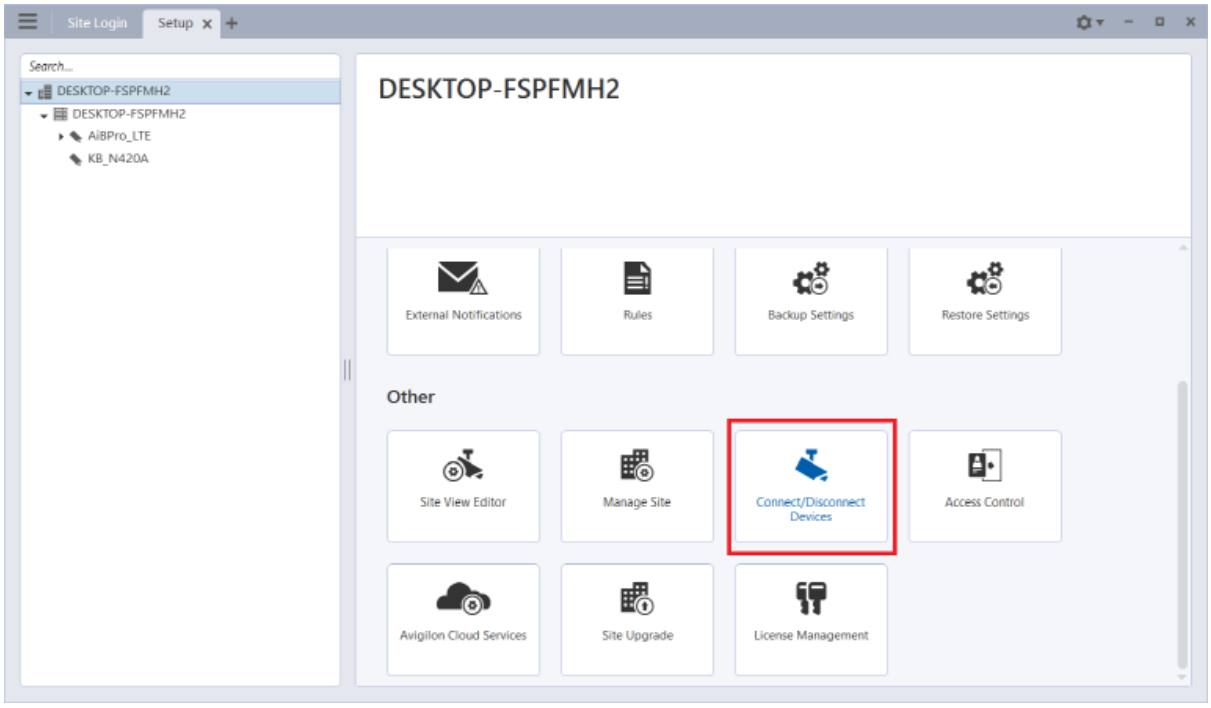


The account created will need permissions for alarm triggering and bookmarking. In this document, we will select administrator rights.

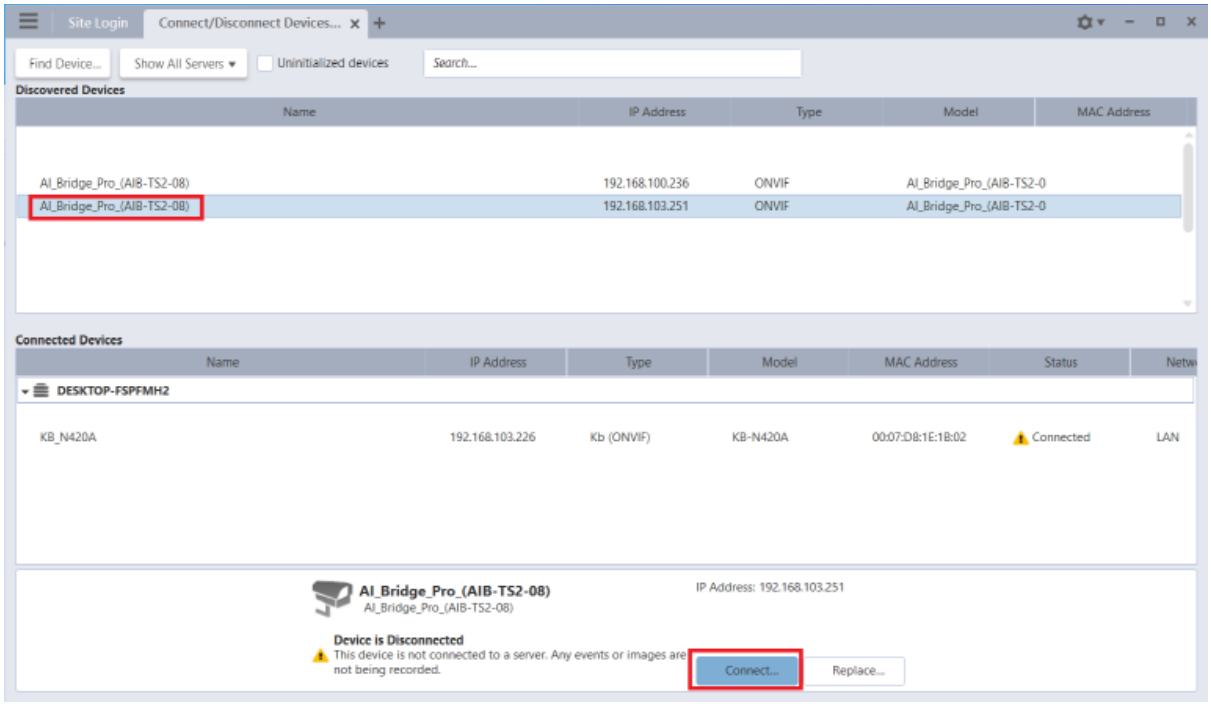


3) Adding the AIBOX to Avigilon ACC VMS.

In the Avigilon ACC Client, select "**Connect/Disconnect Devices**".

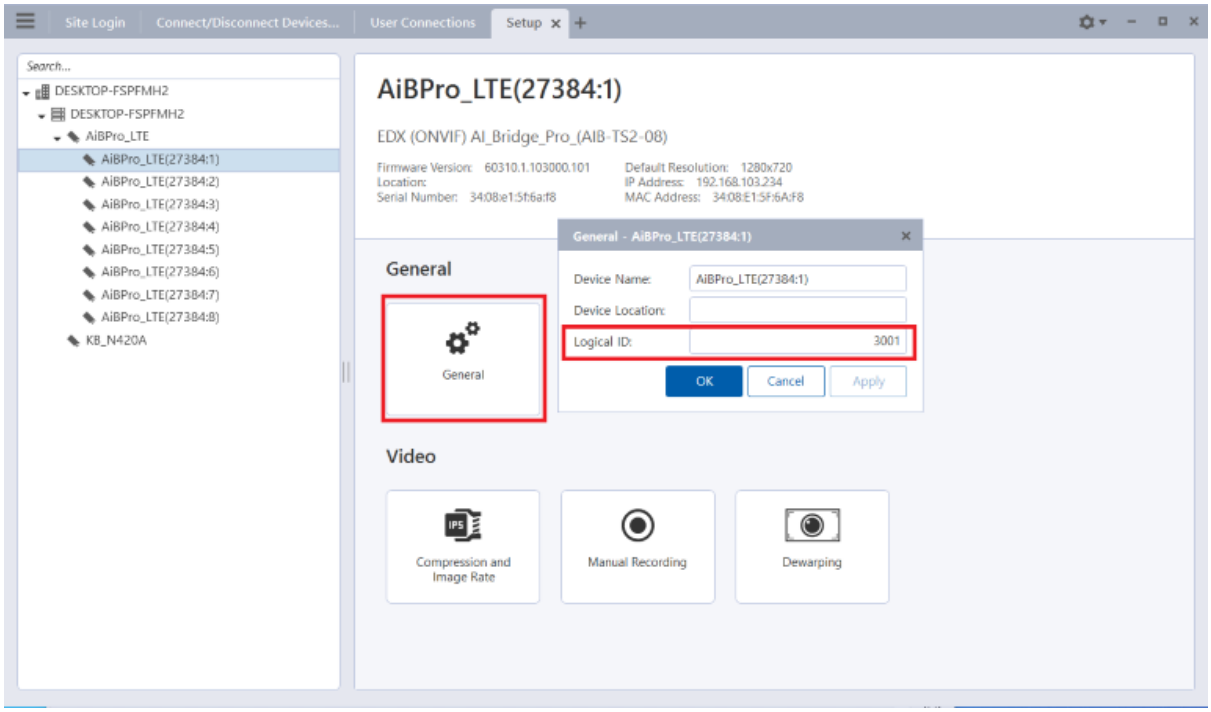


AIBOX operates like an Onvif Device, so it is automatically detected by Avigilon ACC VMS. If the device is not automatically detected, please check your network configuration.

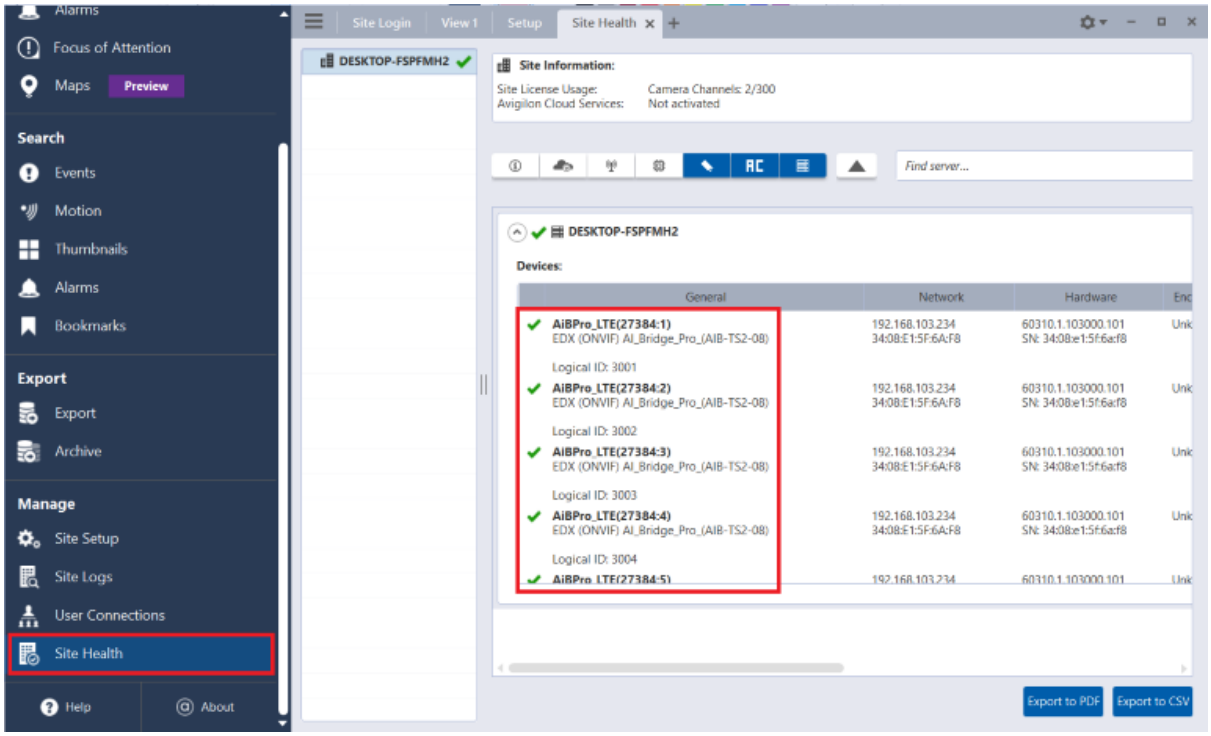


Click on ‘General’ in the properties of each video channel to assign a Logical ID.

This Logical ID is used to link channel information between AIBOX and Avigilon ACC. **Please ensure that it does not duplicate with other channels.**

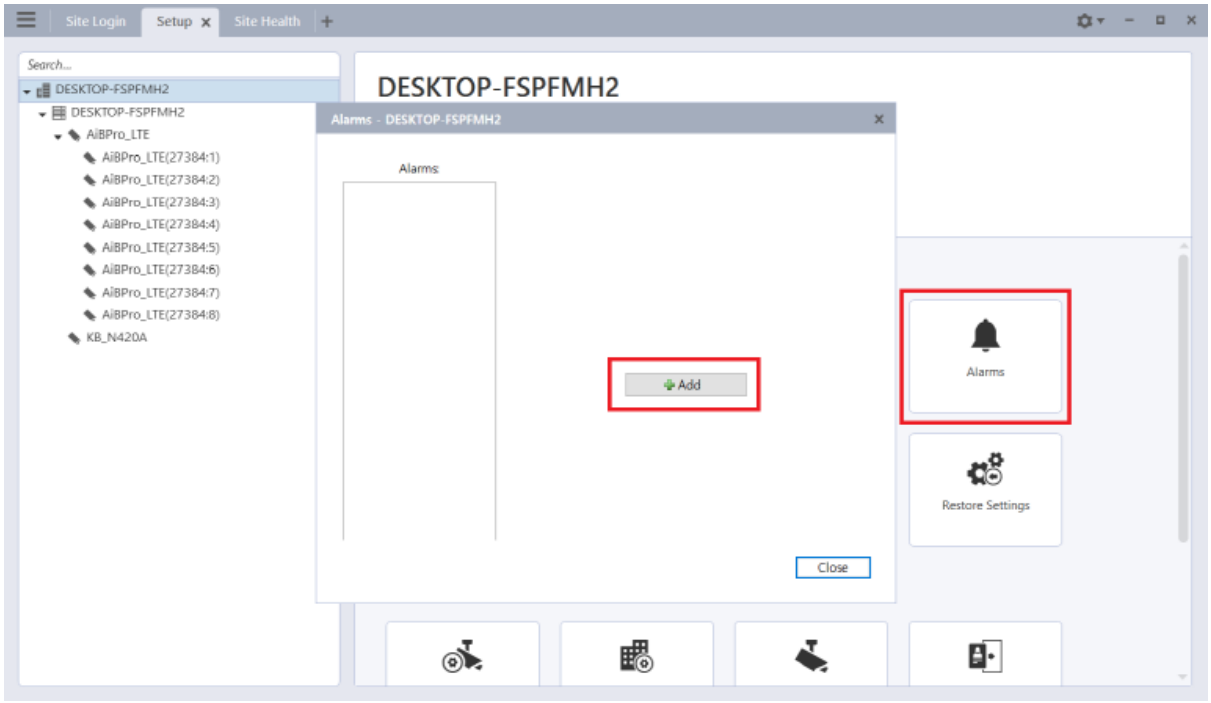


The Logical IDs assigned to each channel can be viewed in the 'Site Health' menu.

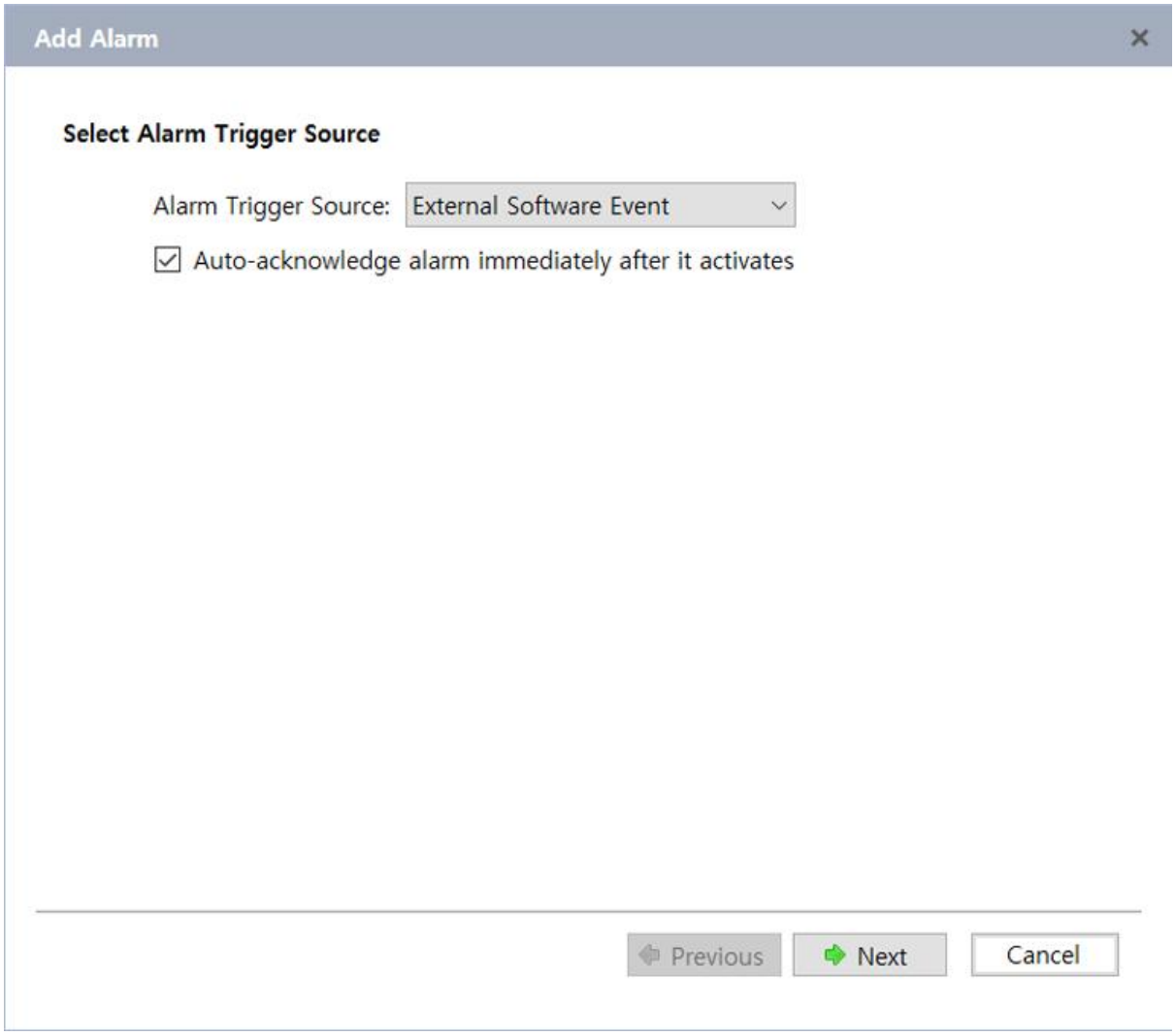


4) Add AI alarm definitions.

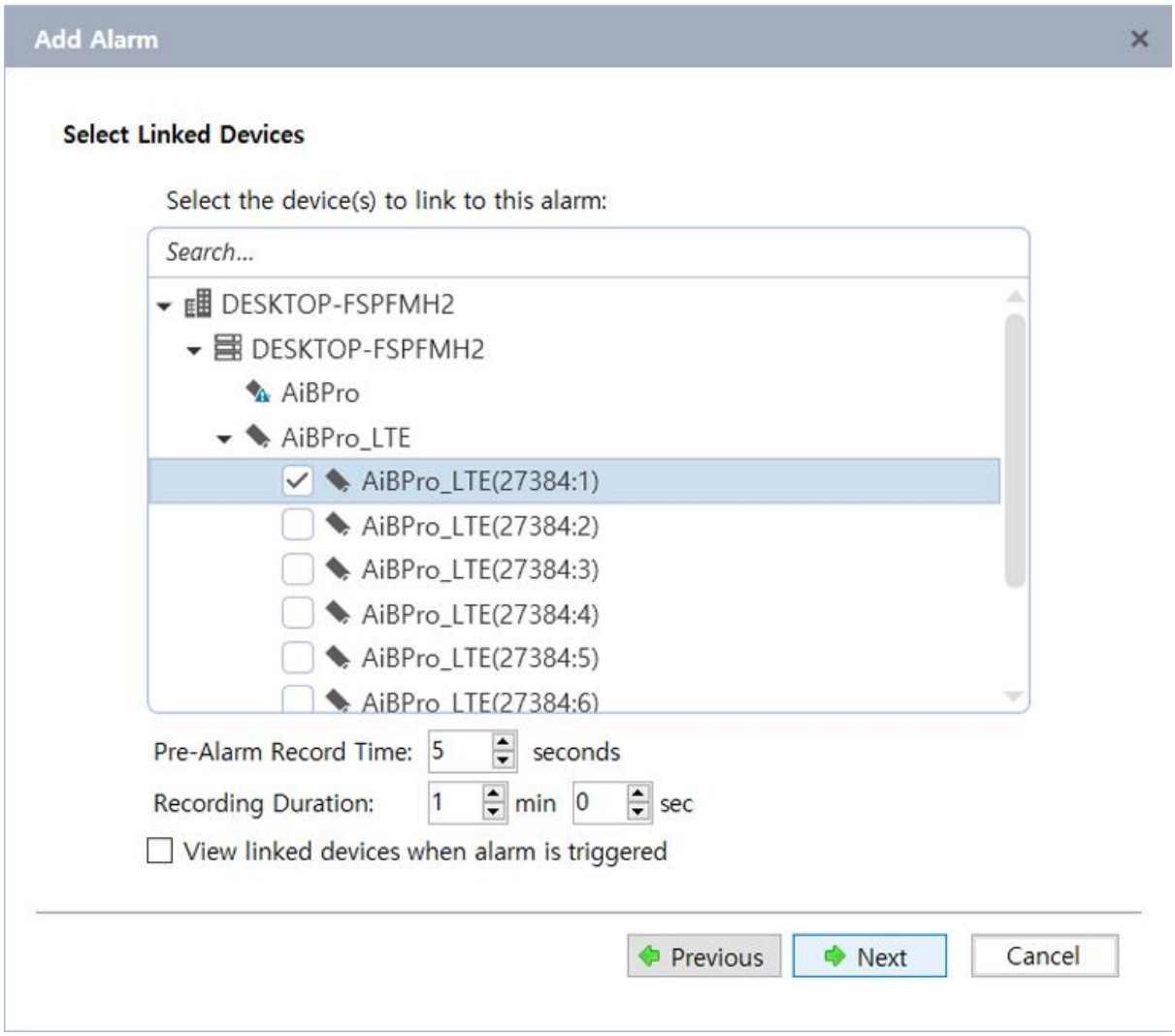
In the Avigilon ACC Client, select "**Alarms**" from General panel



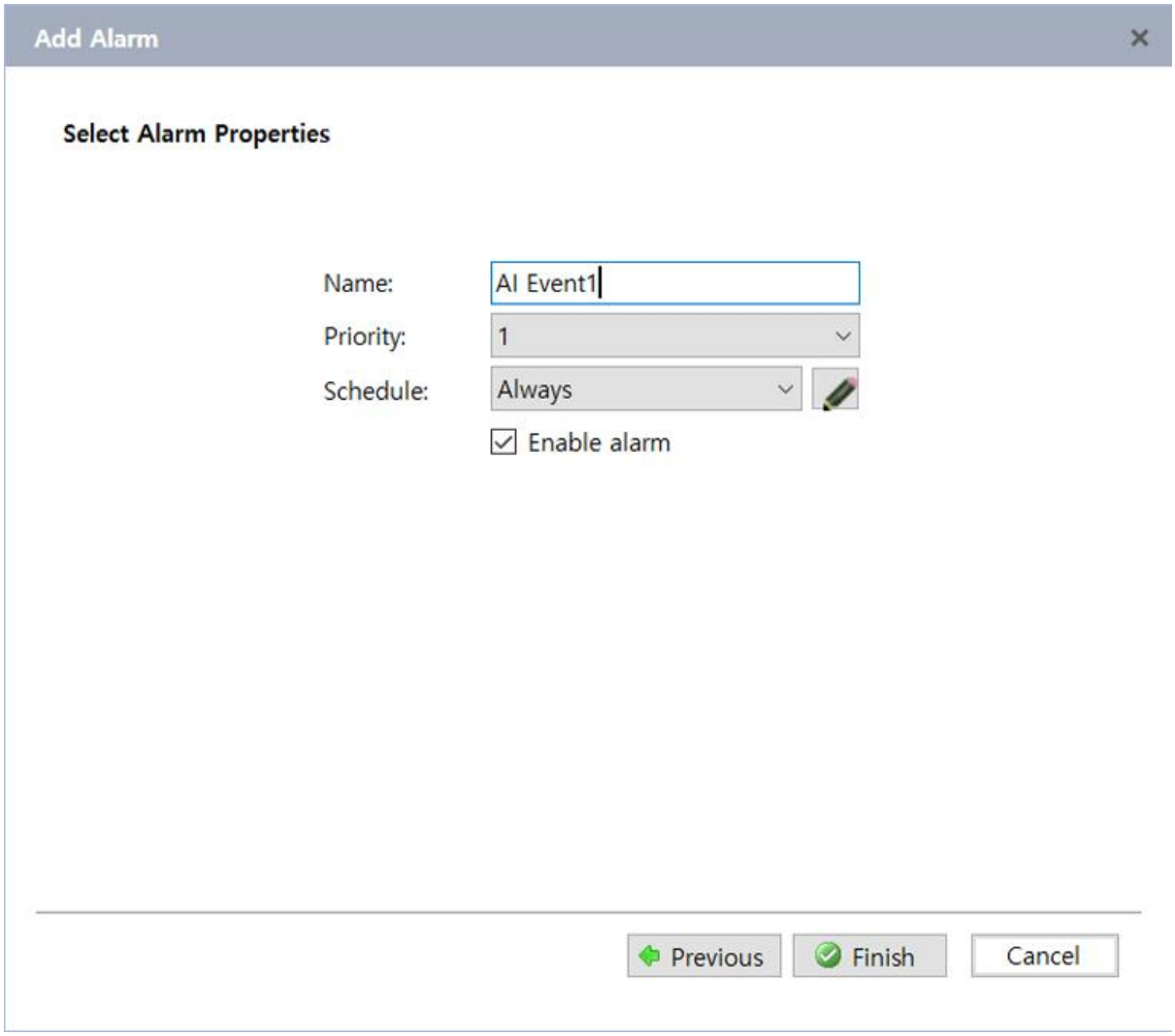
Choose the trigger source “External Software Event”.



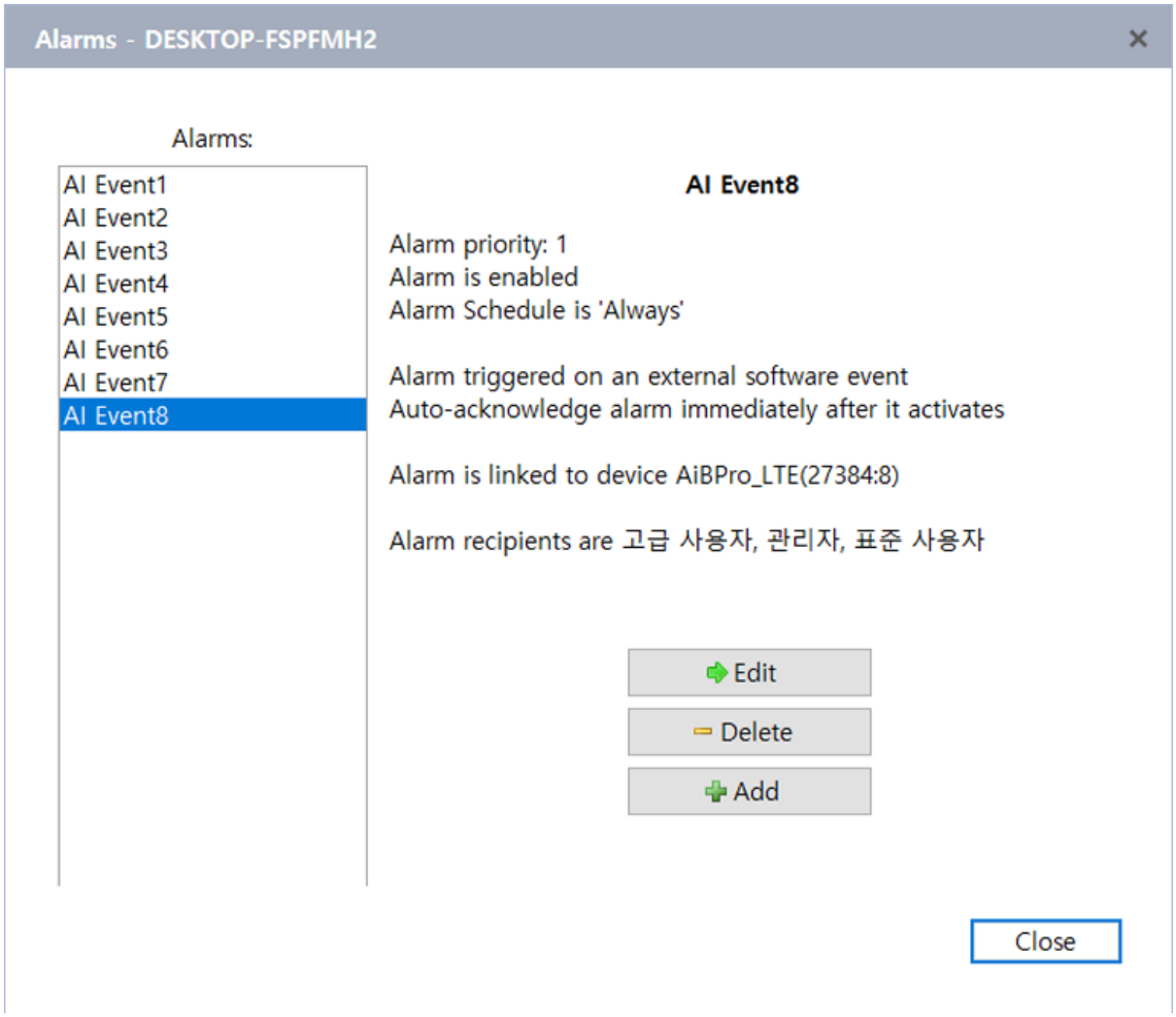
Select the video channel that will be integrated with this alarm.



Enter the event name as "**AI Event1**". This value is an essential key for distinguishing events between AIBOX and Avigilon ACC. It must be entered in the "**Alarm ID**" property in the Avigilon Action handler settings of AIBOX.



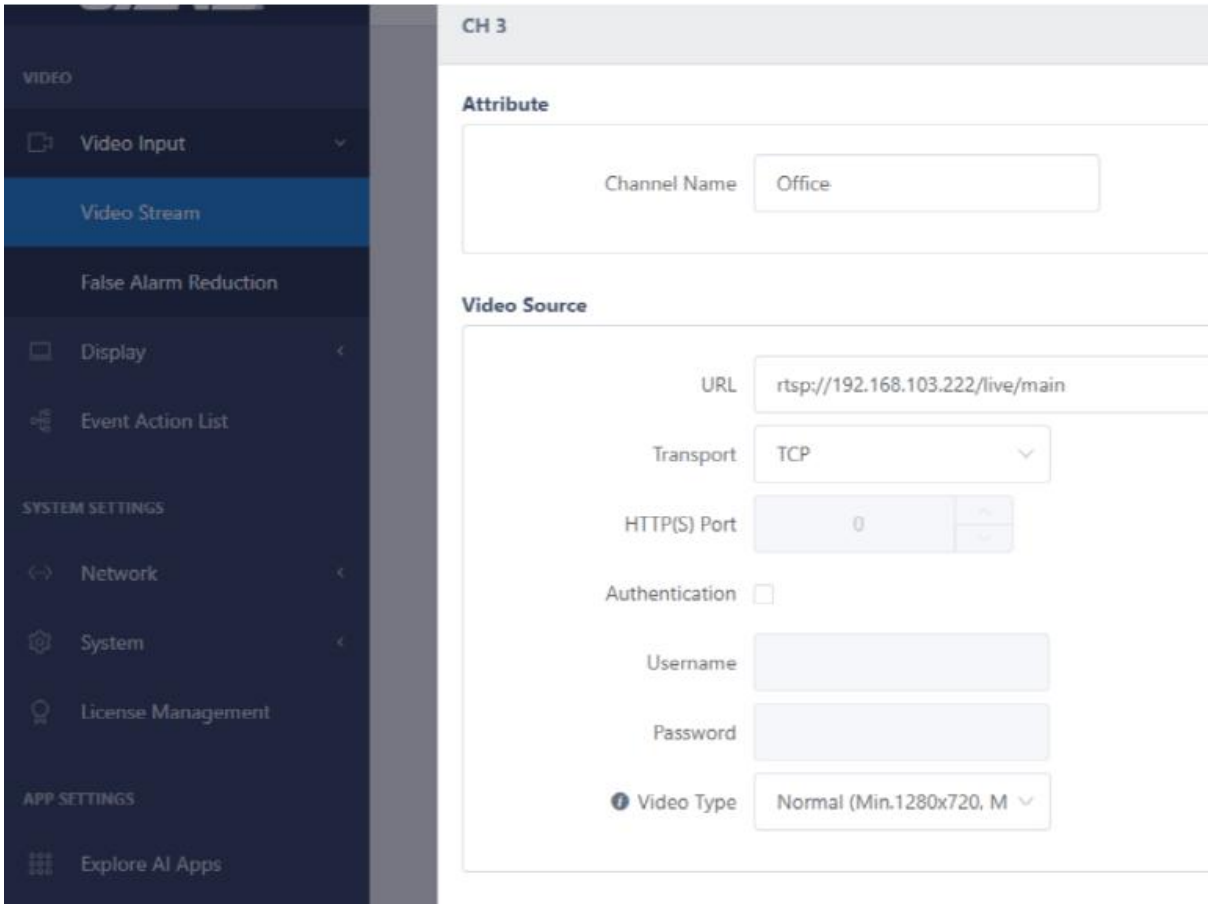
If you want to use different Alarms for each AIBOX channel, you designate video channels for each channel and create alarms sequentially, as shown in the attached example.



2.2 AIBOX Configuration

1) Add Video Stream

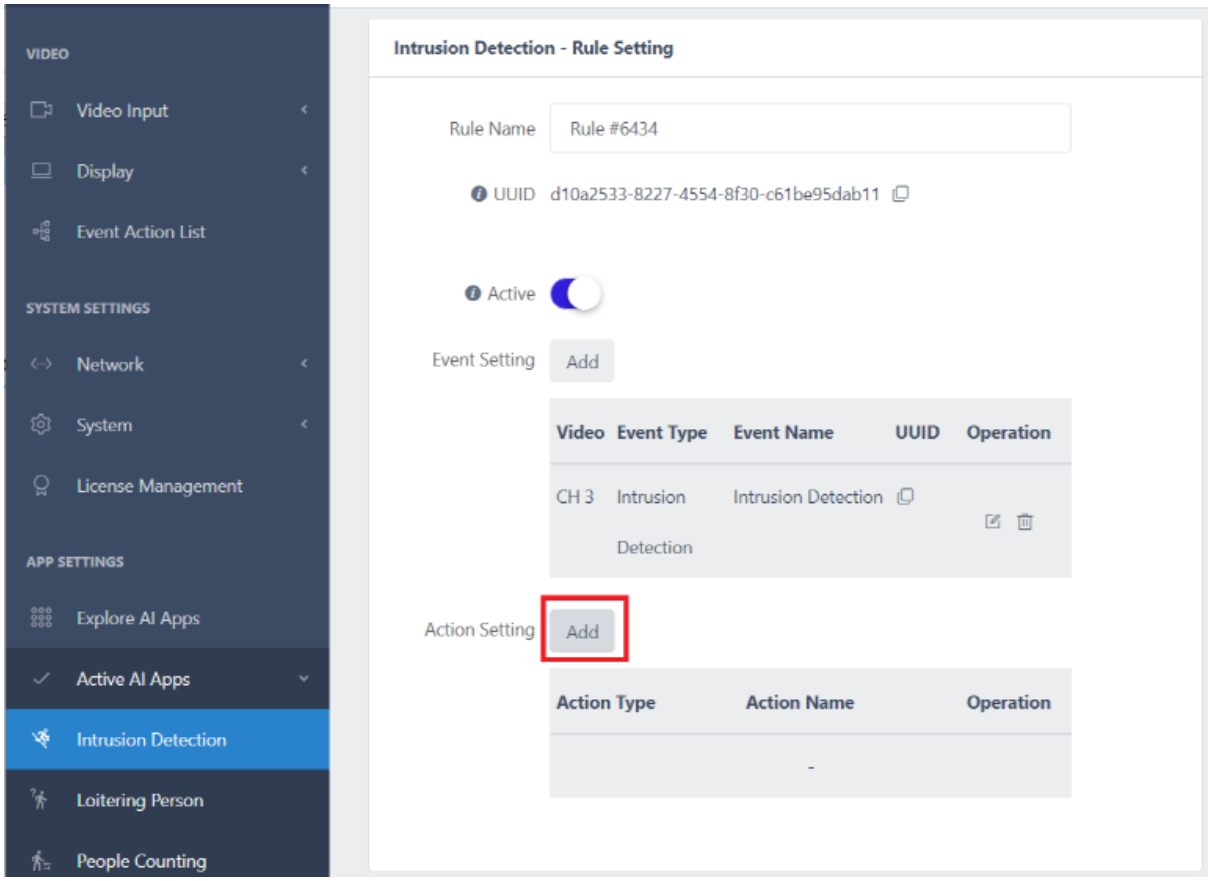
Set (add) the video stream. You can add it either by using an Onvif device search or by directly adding the IPCAM RTSP stream address.



2) Set up the AI App

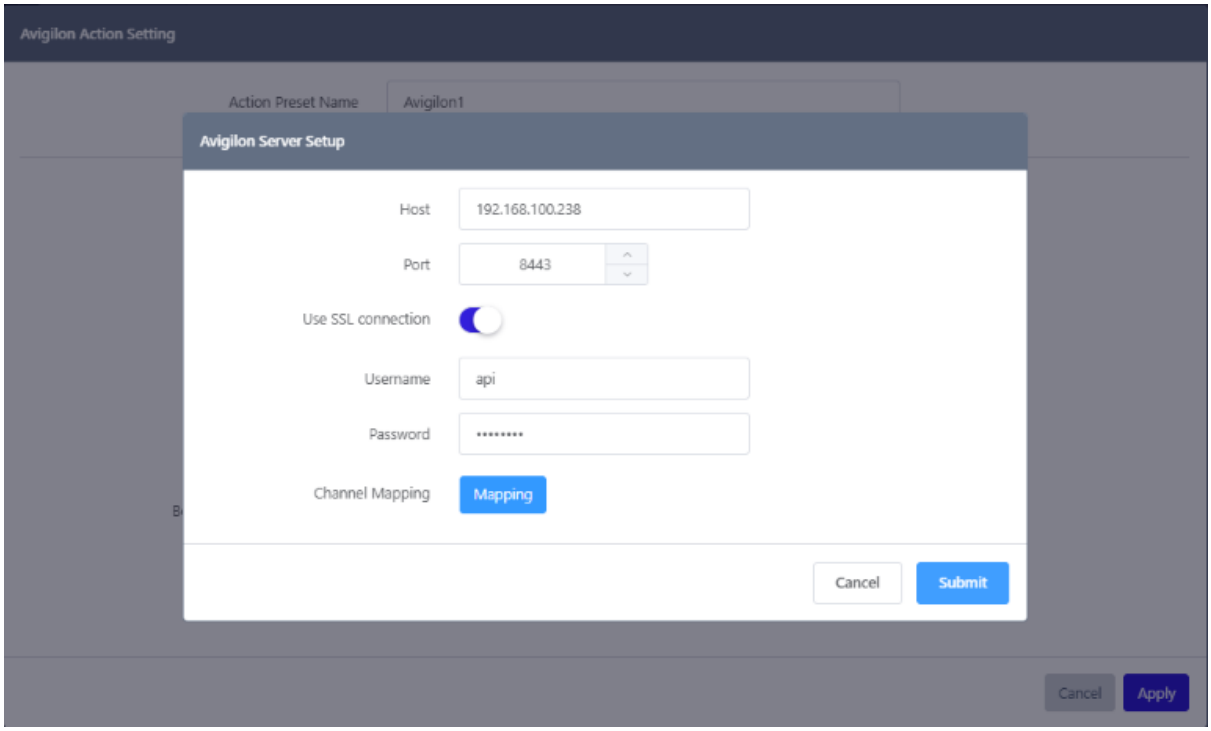
Select the desired AI App and set the AI event for the channel.

In the Actions Setting, click the Add button to add the Avigilon action handler.



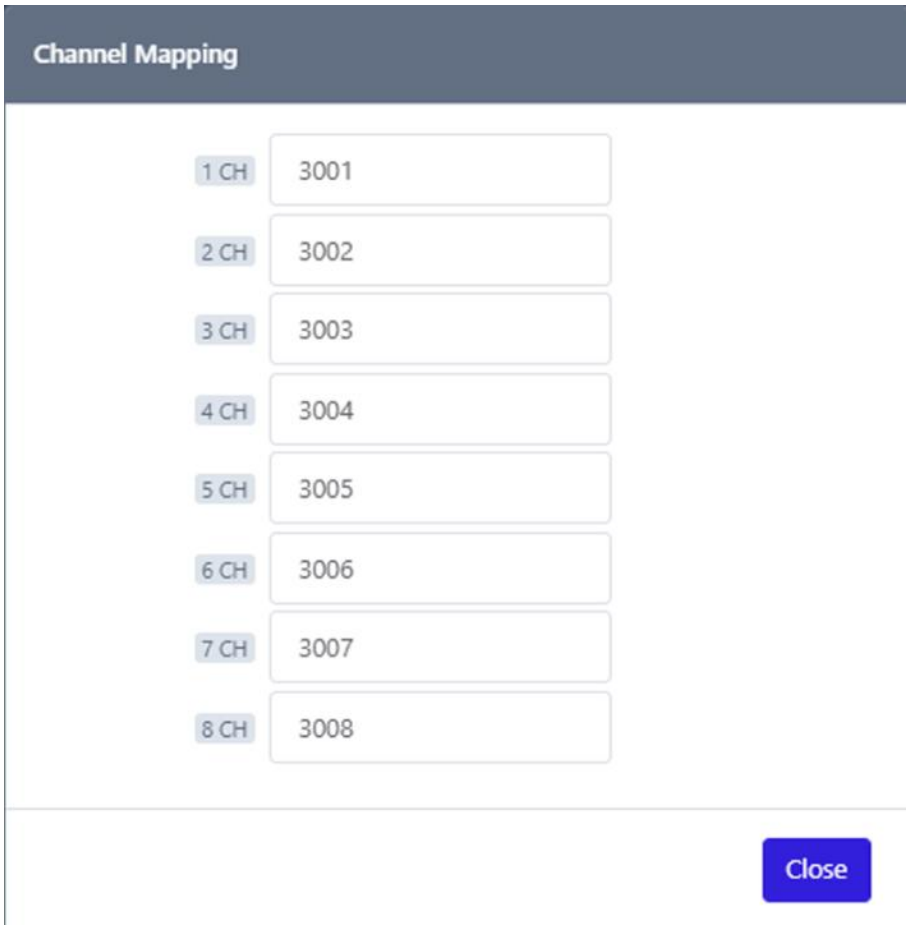
3) Enter the Avigilon ACC VMS Server Information

Enter the IP address of the Avigilon ACC VMS and other server information. Then click the channel "**Mapping**" button.



Enter the Camera Logical ID of Avigilon ACC VMS.

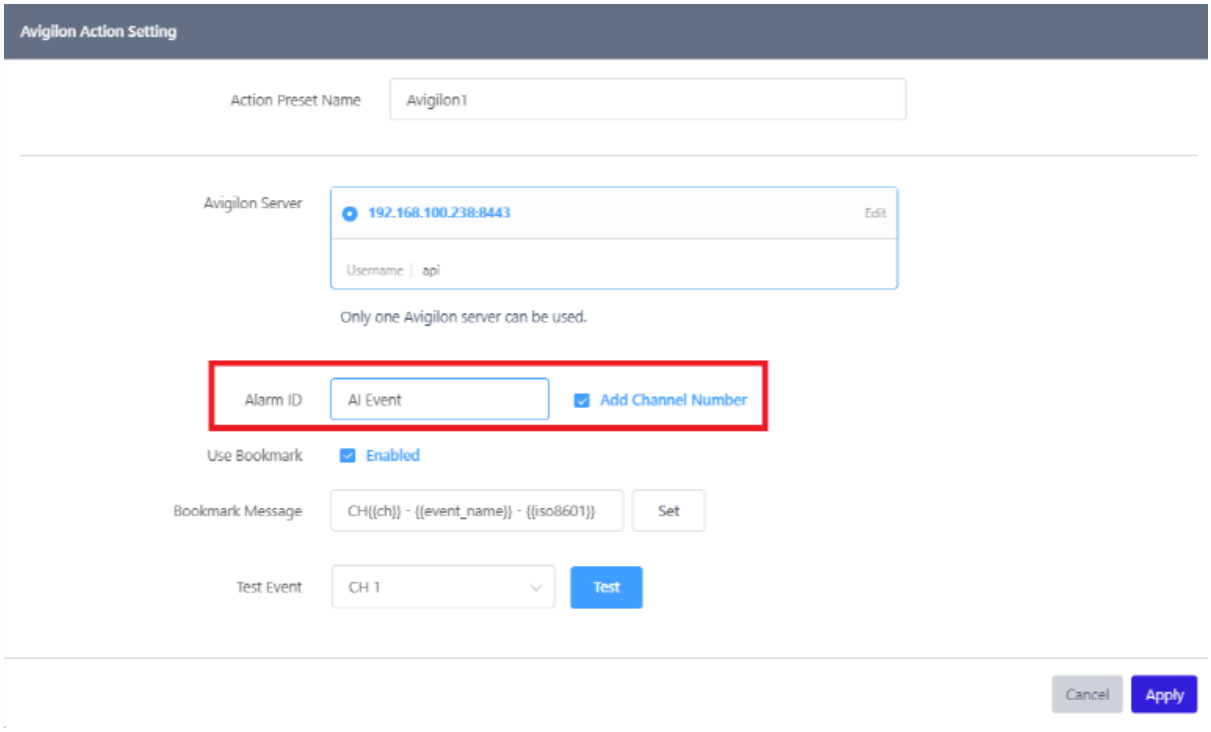
Note: If you enter the IPCAM's Logical ID information instead of the AIBOX's Logical ID in the camera mapping information, it operates as the Case2 integration type.



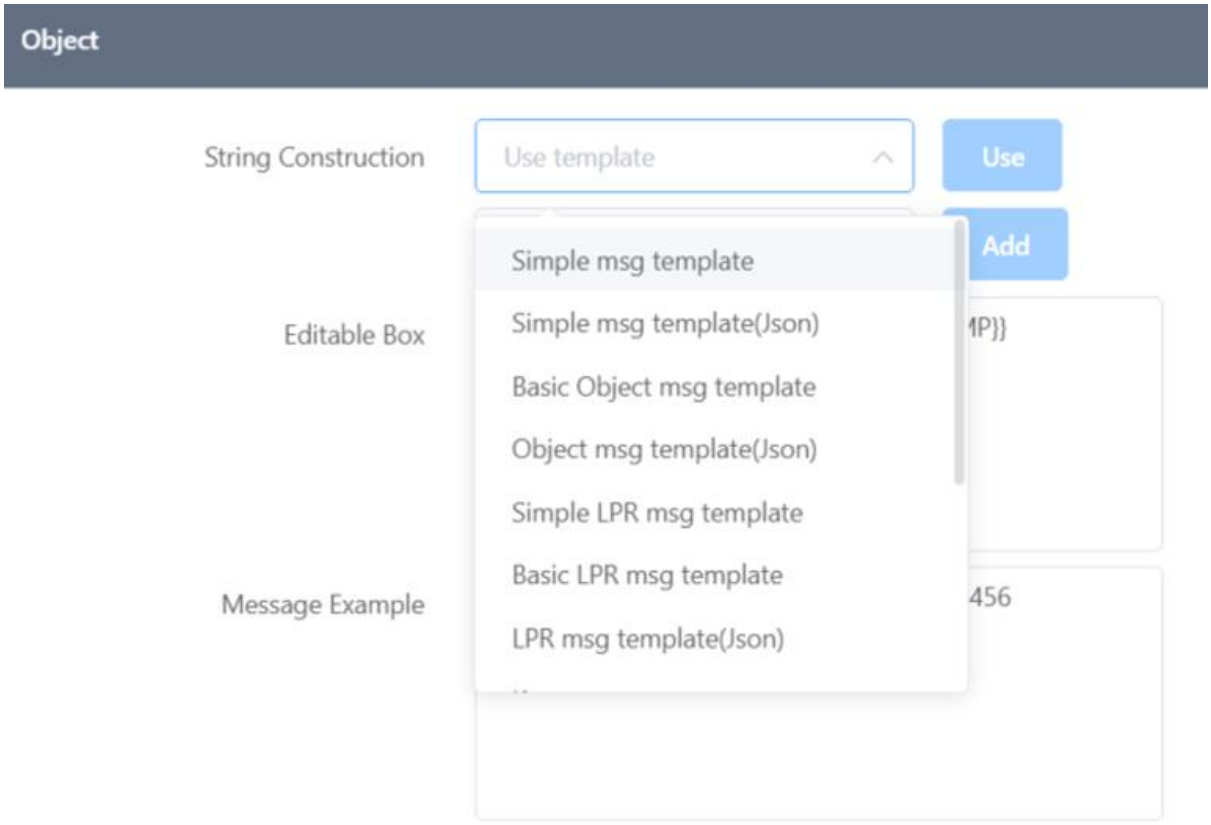
For the "Alarm ID" property, input the name of the "Alarm" that you added in Avigilon ACC. In this guide, we have entered it as "**AI Event**".

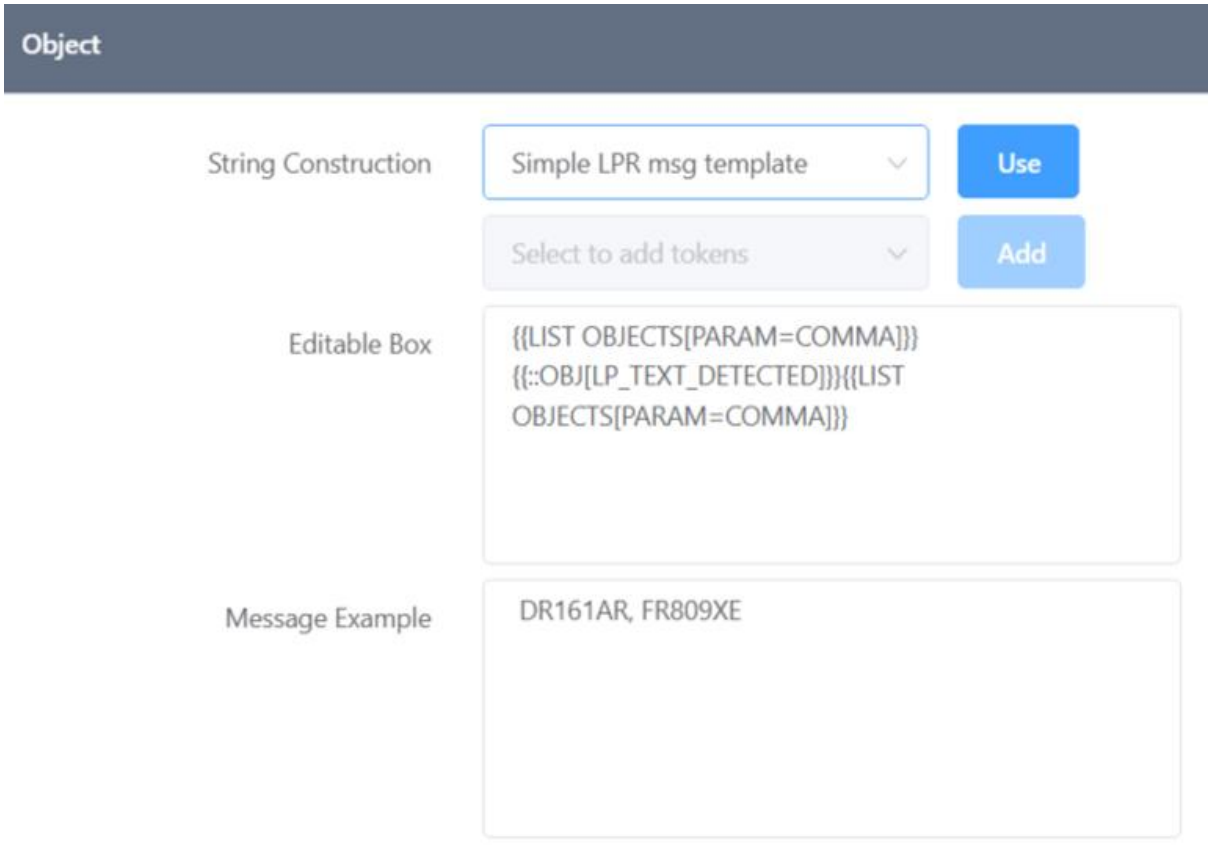
If you select 'Add Channel Number,' the channel number will be automatically added to the Alarm ID.

For example) Channel 1: AI Event1, Channel 2: AI Event2, Channel 8: AI Event8



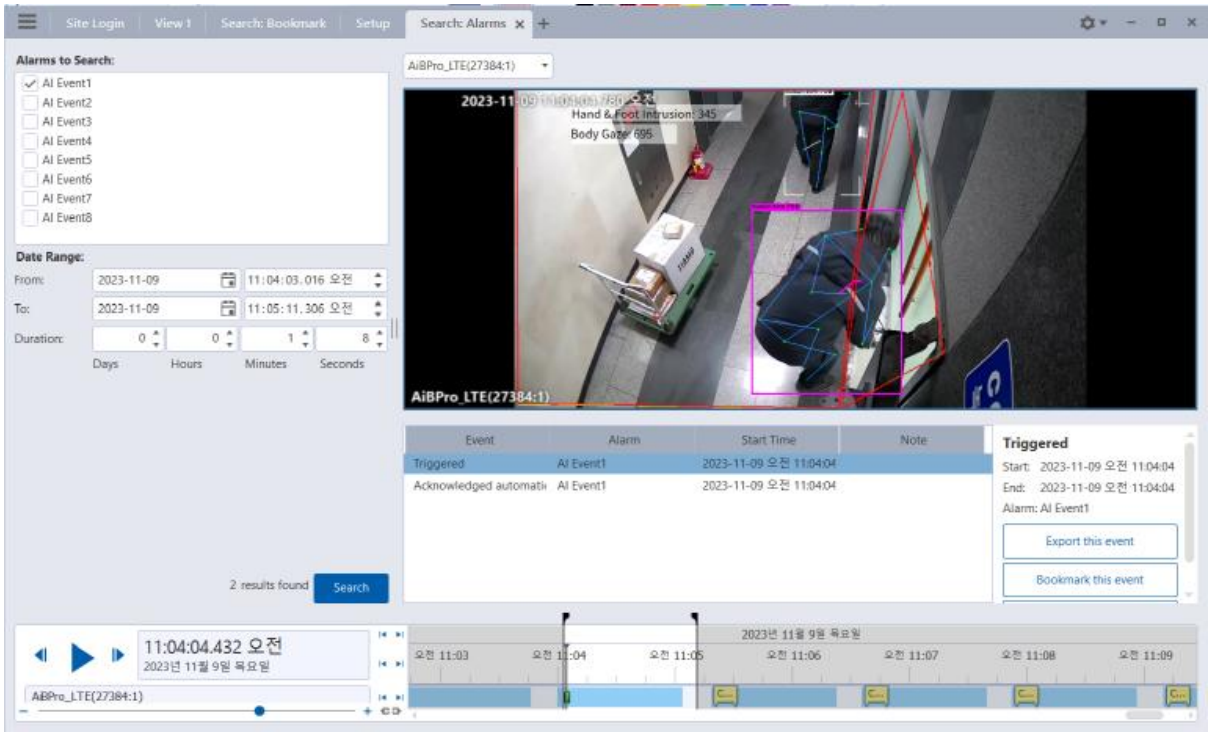
The Bookmark Message field can be utilized in various ways. You can enter event texts, LPR information, etc., so you can send additional information in the Avigilon ACC VMS.



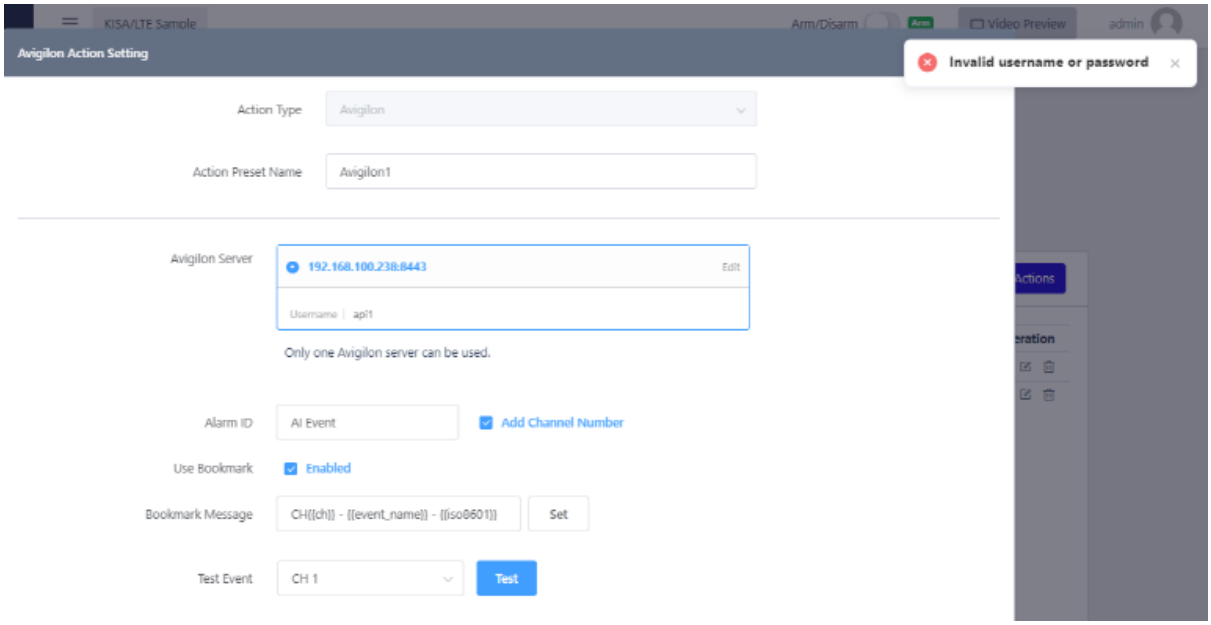


Note: If you want to set the Object property differently for each AI App, you can create a separate Avigilon Action handler for each AI App.

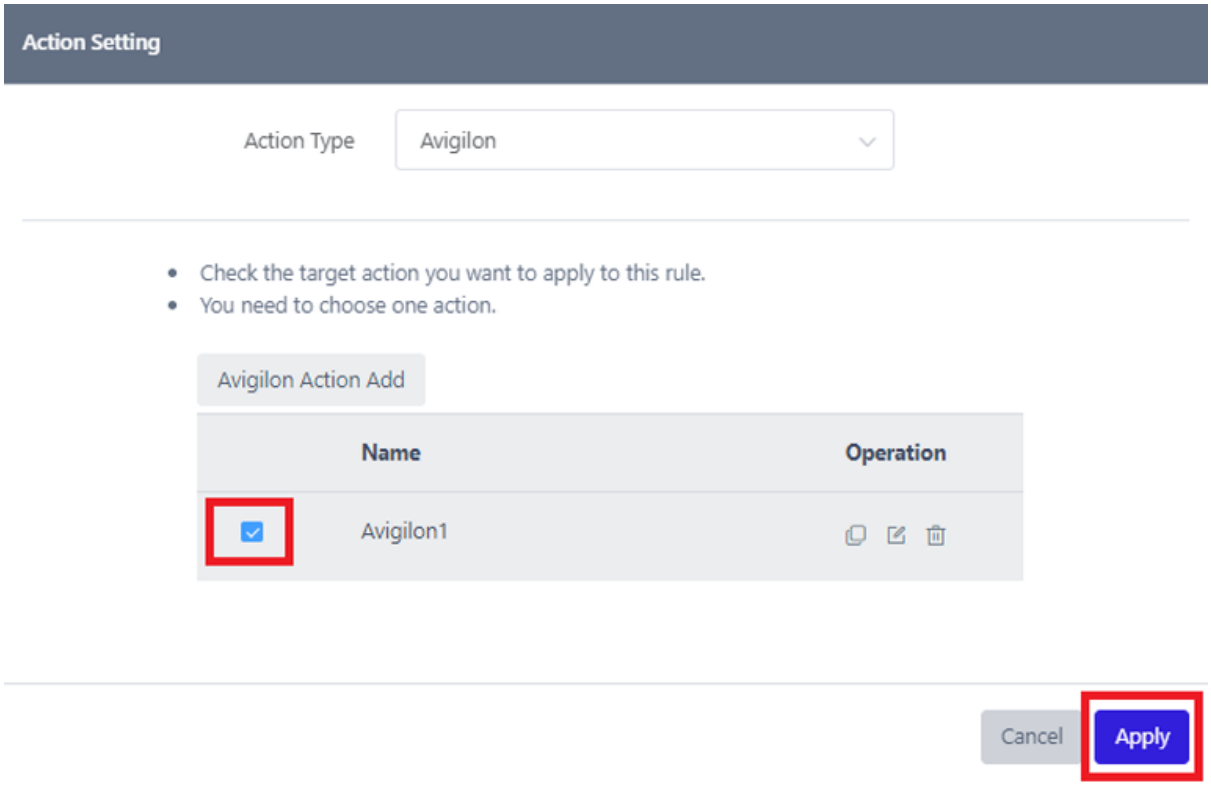
By pressing the “Test” button, you can check the Test Event in the Avigilon ACC Client.



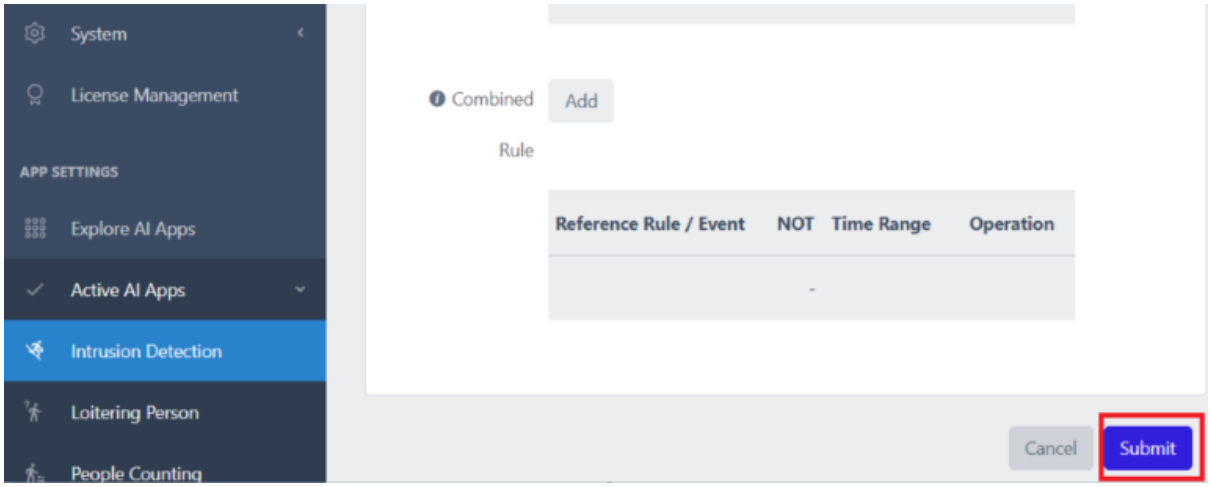
If the test fails, please refer to the error message that appears at the top right of the screen and check the settings. You can verify various issues such as VMS connection failure, authentication failure, incorrect Alarm ID, or incorrect Logical ID of the video.



If the event test is successful, check the “Activate Avigilon action handler” checkbox and press the “Apply” button to save the handler settings.



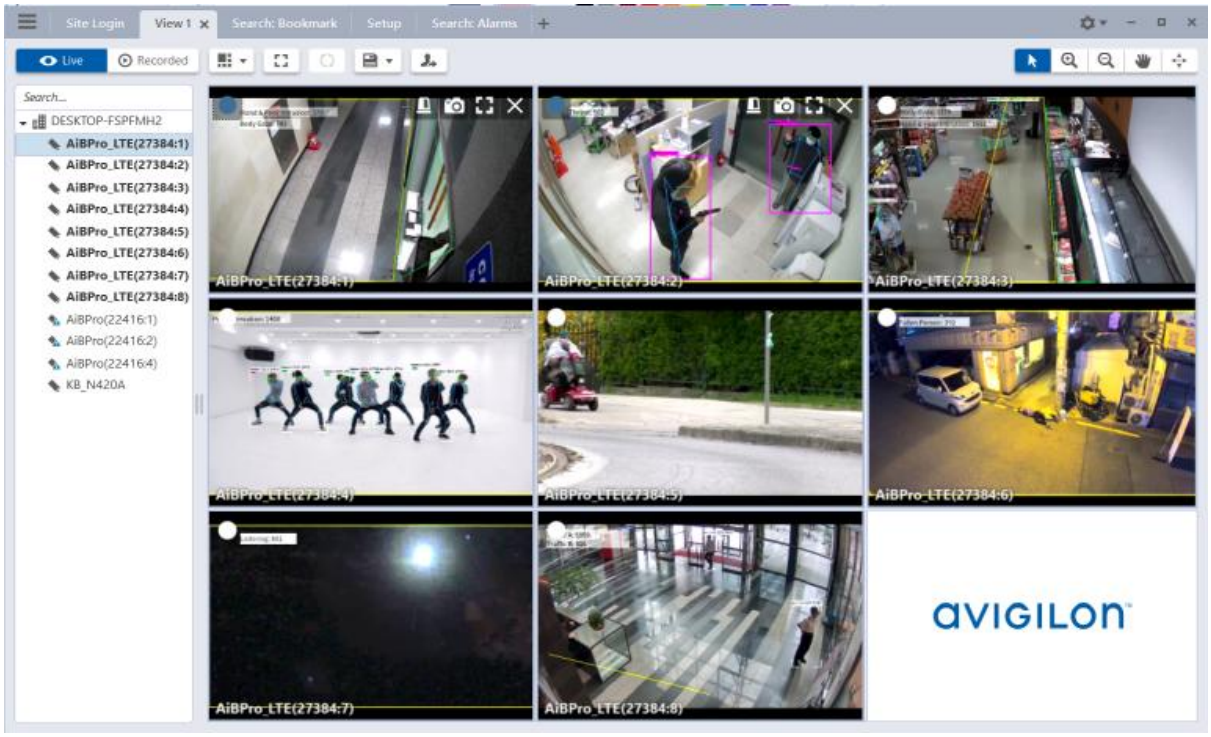
Finally, press the “Submit” button located at the bottom of the AI App settings to save all configurations.



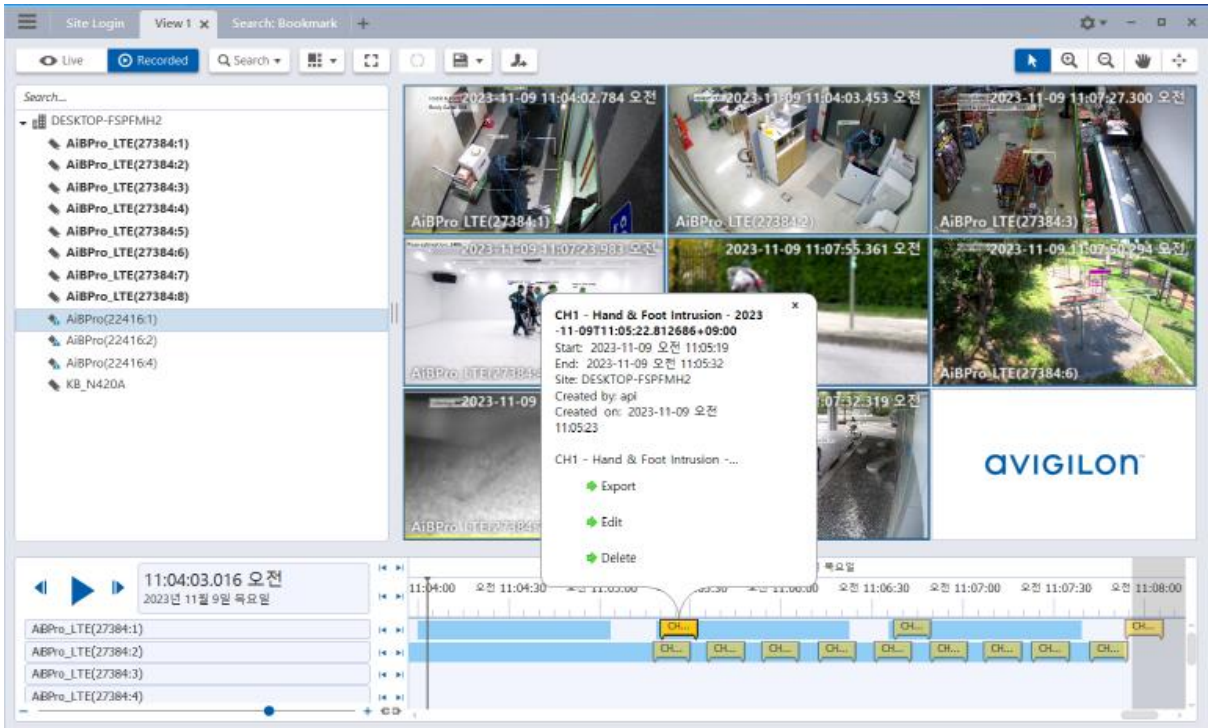
3. Demo

3.1 Live/Recorded

In the live view of Avigilon ACC, you can check object recognition information through the annotated video provided by AIBOX, and a pink BBox appears when an event occurs.

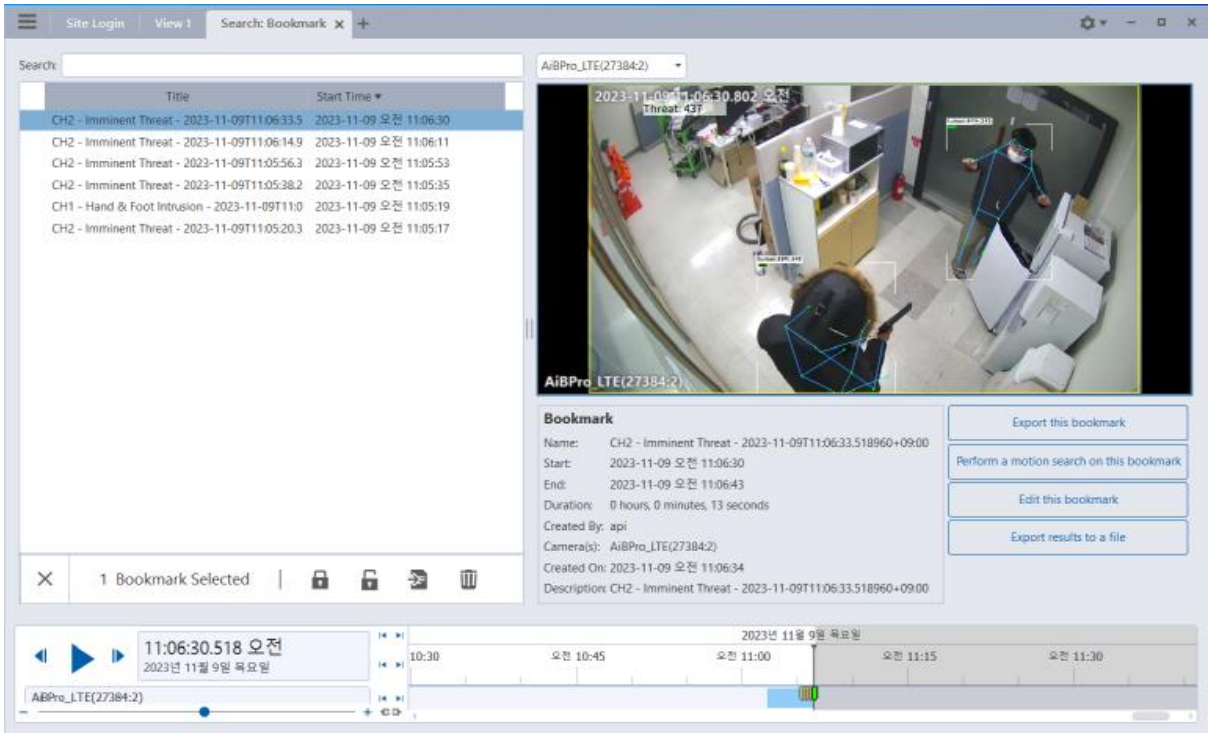


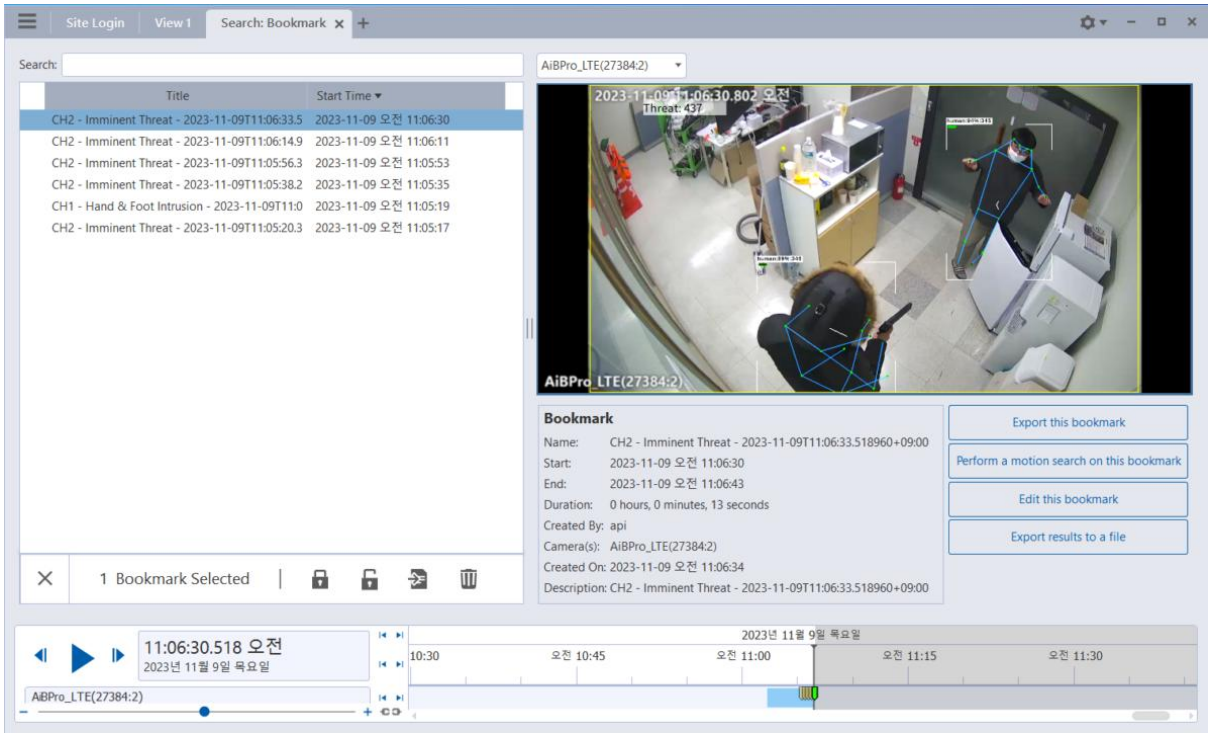
In the recorded data screen of Avigilon ACC, when an AI Event occurs, a bookmark icon appears on the timeline information at the bottom of the screen, and by clicking on the bookmark, you can view the details of the AI Event.



3.2 Search

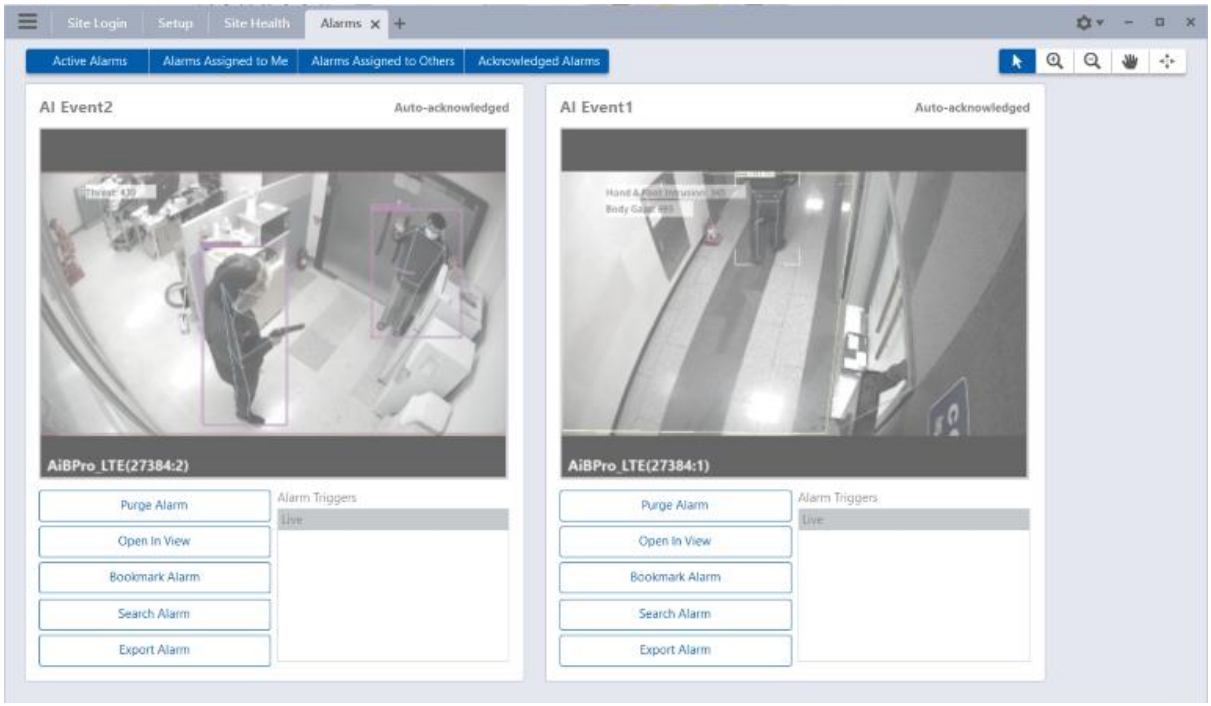
In the bookmark search screen, you can search for AI Events that have been automatically bookmarked when they occur. By utilizing the Bookmark Message in AIBOX's Avigilon settings, you can dynamically generate various information. For example, using the LPR (License Plate Recognition) information template, you can find the license plate information through bookmark search.





3.3 Alarm Manager

In the Alarm Manager, by clicking on an individual alarm, you can check detailed event occurrence information with recorded video.



exacqVision Integration Guide

1. Introduction

1.1 Prerequisites

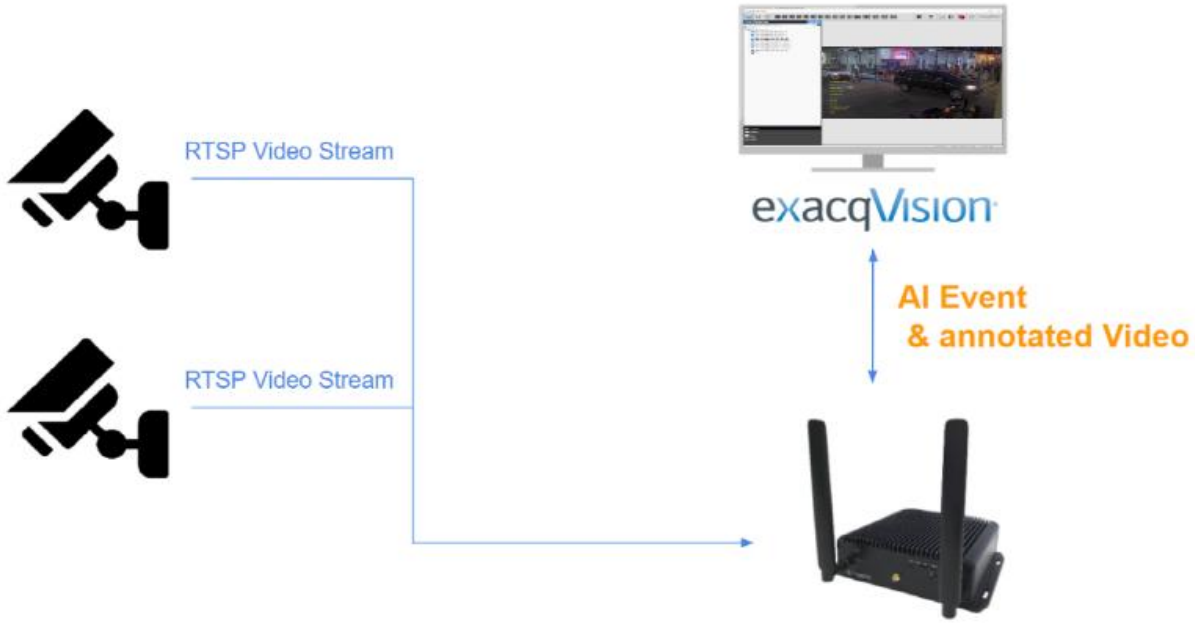
- AIBOX FW version 103708 or higher.
- exacqVision Client 24.06.1.0 higher.

1.2 Learn about integration architecture

There are two ways to integrate AIBOX with exacqVision VMS:

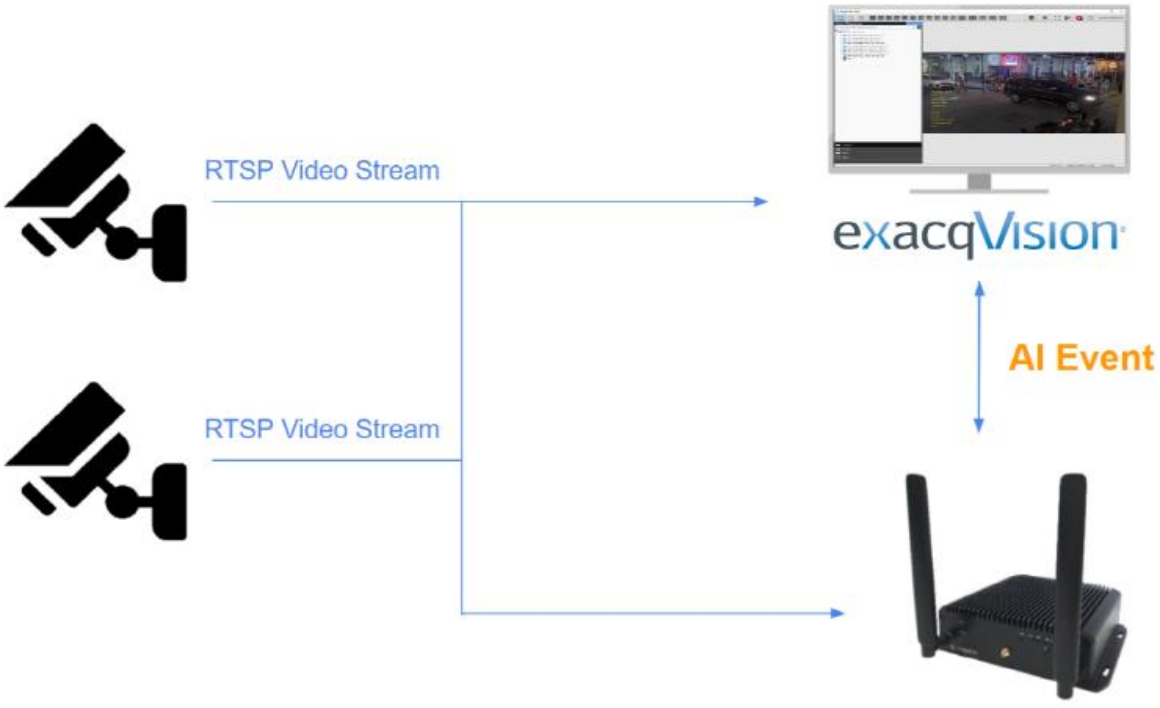
1) Case 1

AIBOX receives the RTSP video stream from the IPCAM and processes it to provide annotated videos and event data after AI analysis. The video is transcoded to include object recognition data, bounding boxes, zone information, and more.



2) Case 2

Both AIBOX and exacqVision VMS simultaneously receive the RTSP stream from the IPCAM. AIBOX sends the AI analysis events directly to XProtect VMS and can also source the RTSP stream from exacqVision VMS instead of directly from the IPCAM.



Among Case1 and Case2, this guide will explain how to integrate using Case1.

2. Configuration

To integrate events between AIBOX and exacqVision, exacqVision Serial port configuration and AIBOX configuration are required. The following explains each configuration method.

2.1 exacqVision Configuration

2.1.1 Adding Device

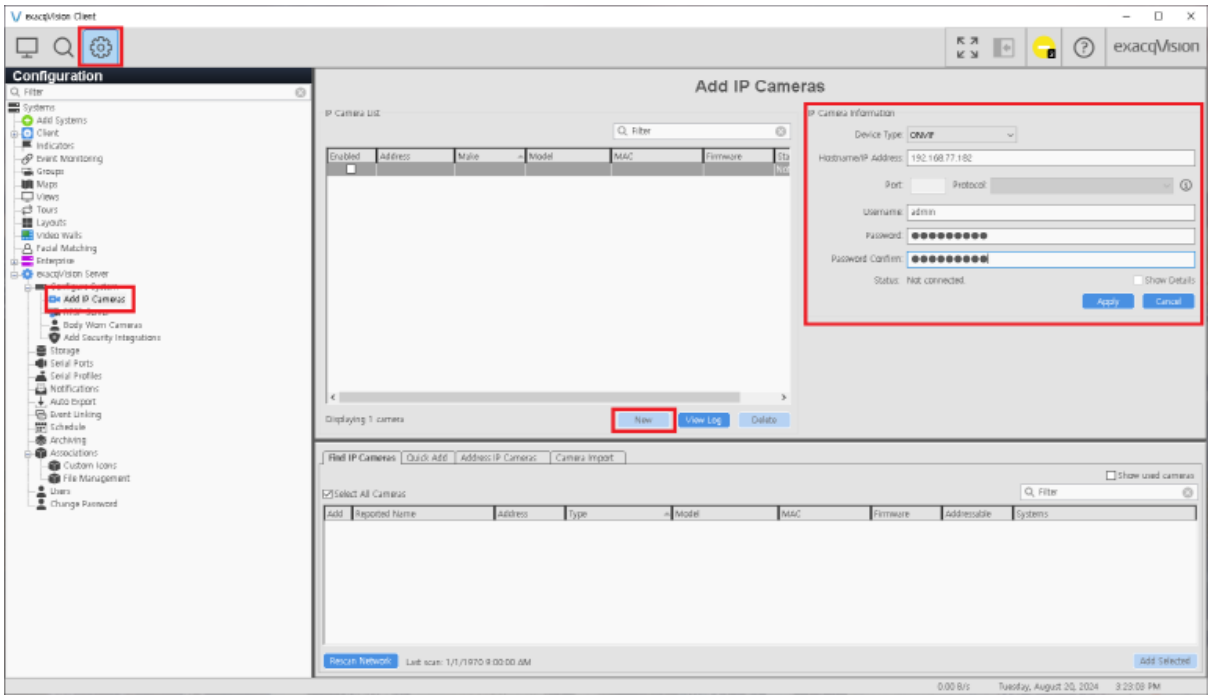
To use the annotated video, you must first add the device. The following explains how to add the device.

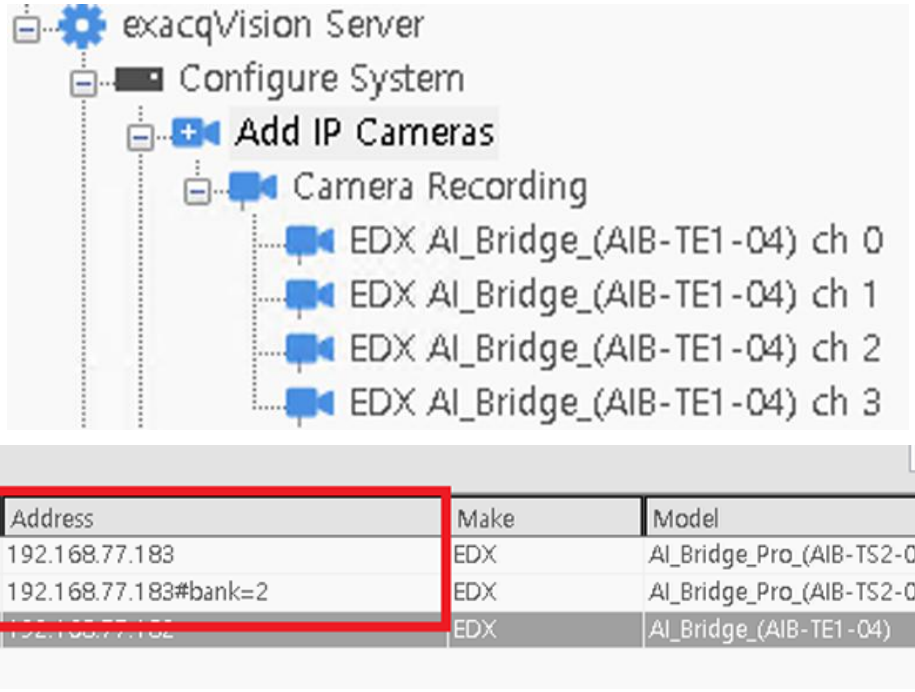
If you are not using the annotated video, you can skip this session.

Note. We have created this guide using Case1 because we prefer annotated video.

Note. To successfully add the device, the video stream must be input into the AIBOX.

In the exacqVision Client, click ‘Add IP Cameras’ and then press the ‘New’ button to enter the device information and add the device.





Note. When registering an AIBOX with more than 4 channels, please add #bank=n after the IP address. (Example: 192.168.77.182, 192.168.77.182#bank=2, 192.168.77.182#bank=3, 192.168.77.182#bank=4)

2.1.2 Serial Ports Setting

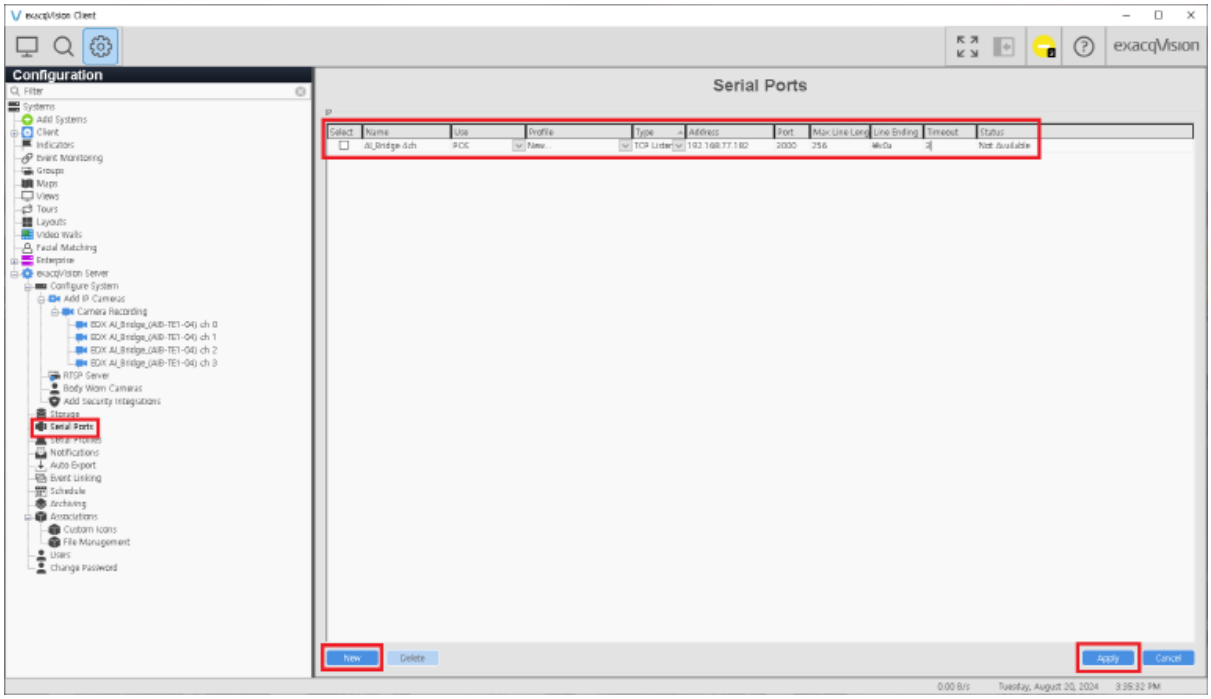
Once the device registration is complete, follow these steps to register the AI Event in exacqVision.

In the Serial Ports tab, click New, then enter your desired value for Name. Set Use to **'POS'**, and Profile to New. For Type, select **'TCP Listener'**, and enter the **AIBOX's IP** in the Address field. Enter the port that you will configure in the AIBOX for the Port field. Set Max Line Length and Timeout appropriately, and enter **'\x0a'** for Line Ending.

After completing the settings, click the Apply button. This will automatically take you to the Serial Profiles tab.

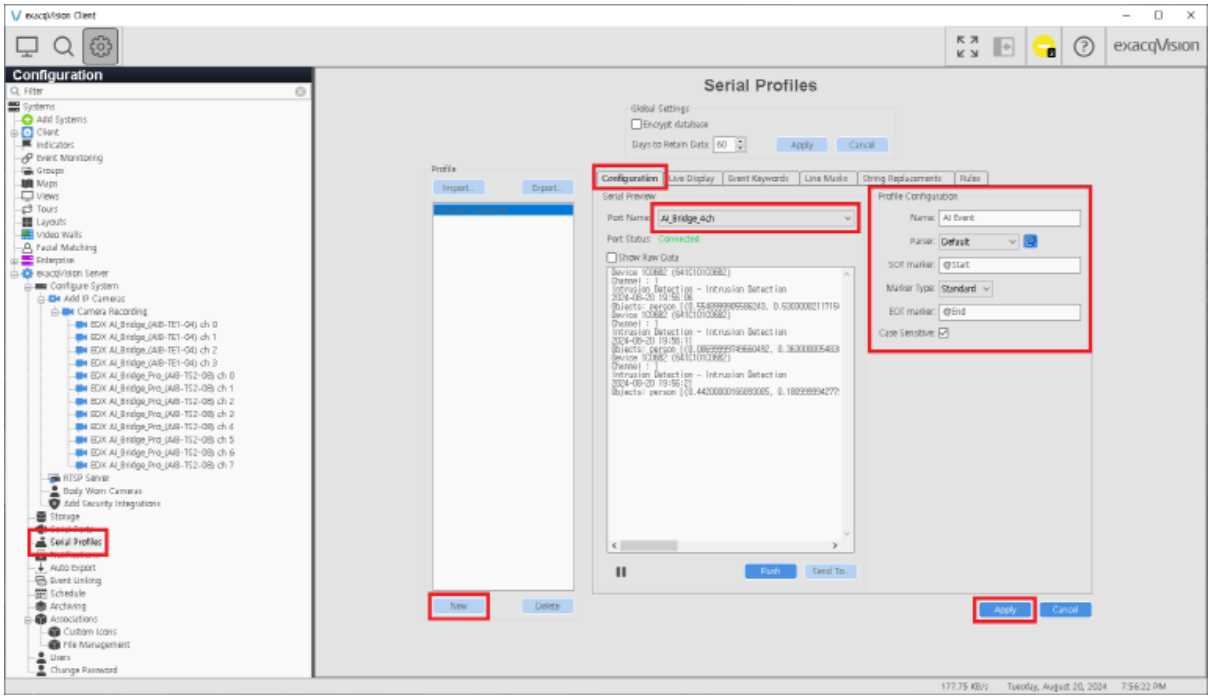
Note: '\x0a' is a hexadecimal code that represents a line break and is specified in the exacqVision manual.

Note. If you have an existing Profile, please select that Profile.



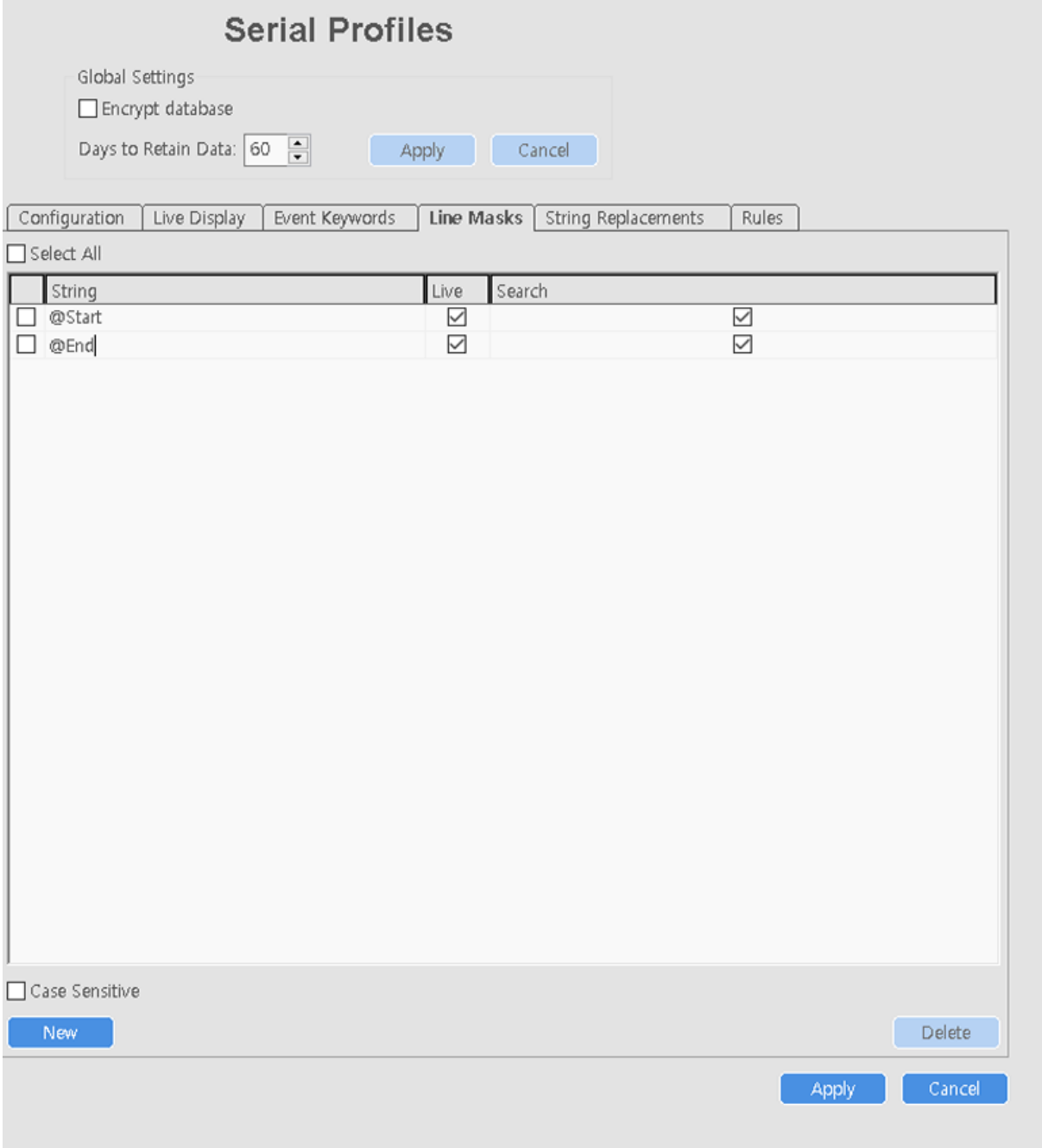
2.1.3 Serial Profiles Setting

In the Serial Profiles tab, click New, then select the Port Name you created earlier. Enter '@Start' in the SOT marker field and '@End' in the EOT marker field, then click the Apply button.



In the Live Display tab, select the background video where the message will be displayed, then drag within the video to choose the location for the message. You can adjust the font settings in the Text Formatting section.

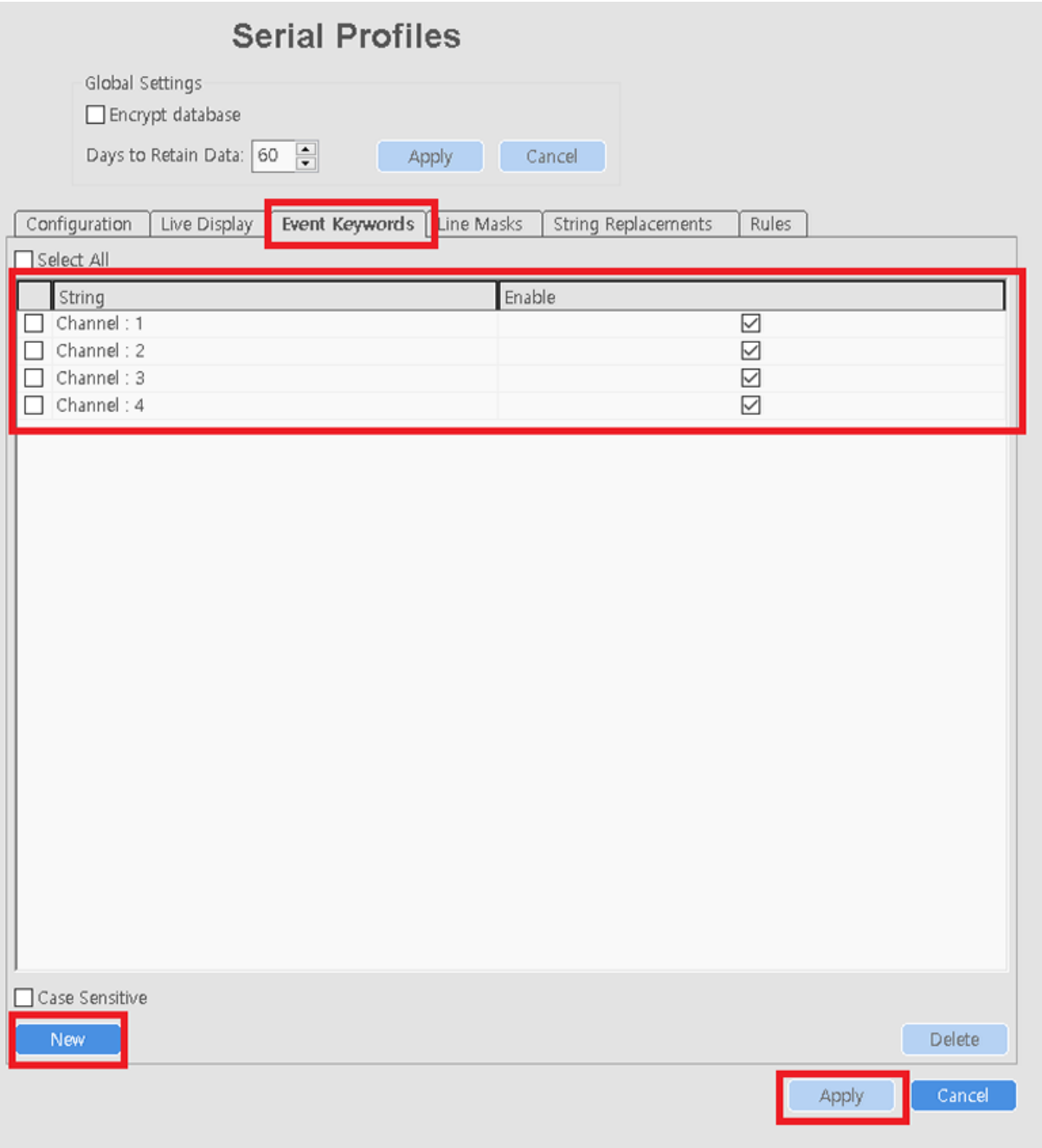
TIP. The exacqVision server port can only use one port, and since exacqVision also only allows one communication per port, all events for a single AIBOX will be received on that port. Therefore, it is recommended to set the Serial Profile's background to None instead of a specific channel.



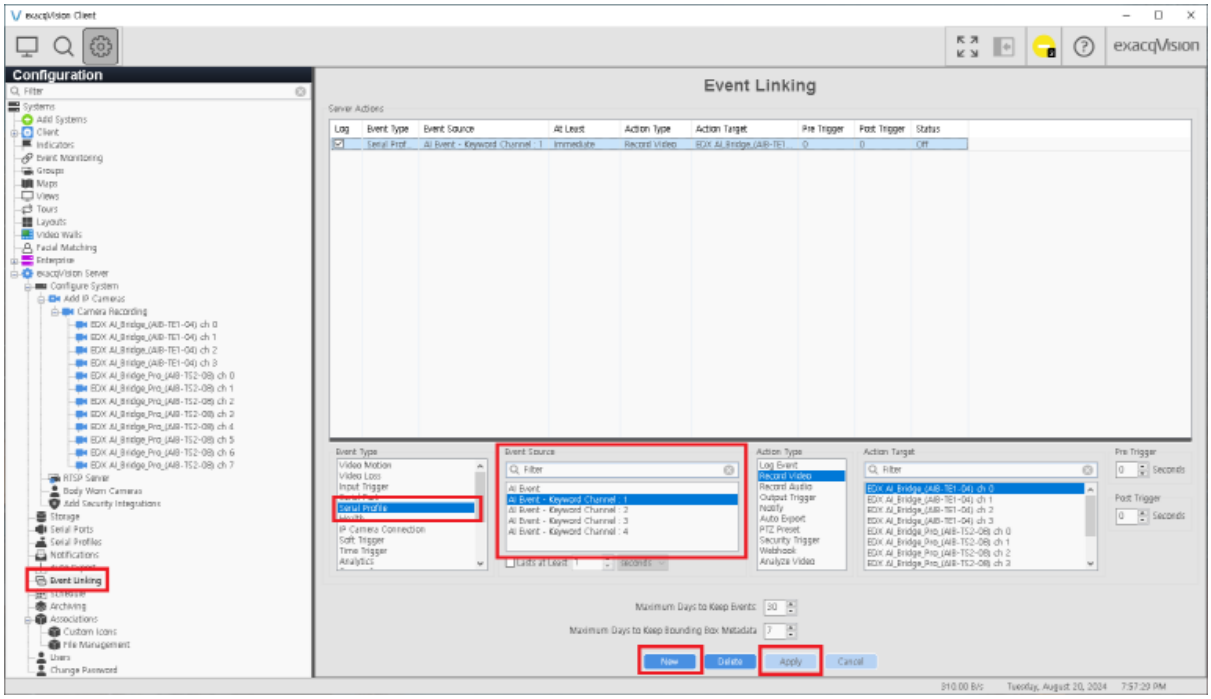
TIP. In the Line Masks, you can add the desired text to ignore specific data.

2.1.4 Event Keywords Setting for Event Linking

In the Serial Profiles tab, go to the Event Keywords section and add the Channel keywords.



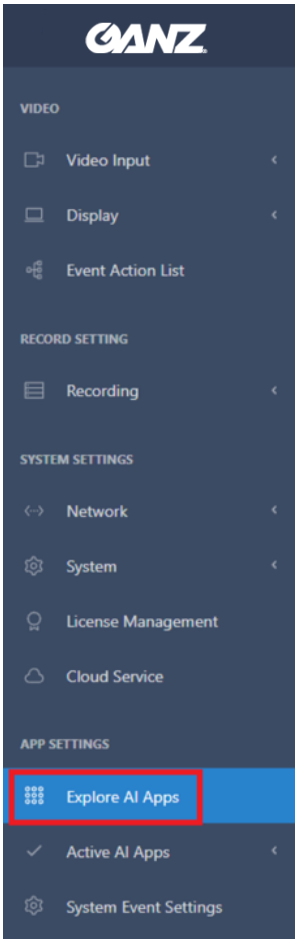
In the Event Linking tab, register the event actions for each channel.



2.2 AIBOX Configuration

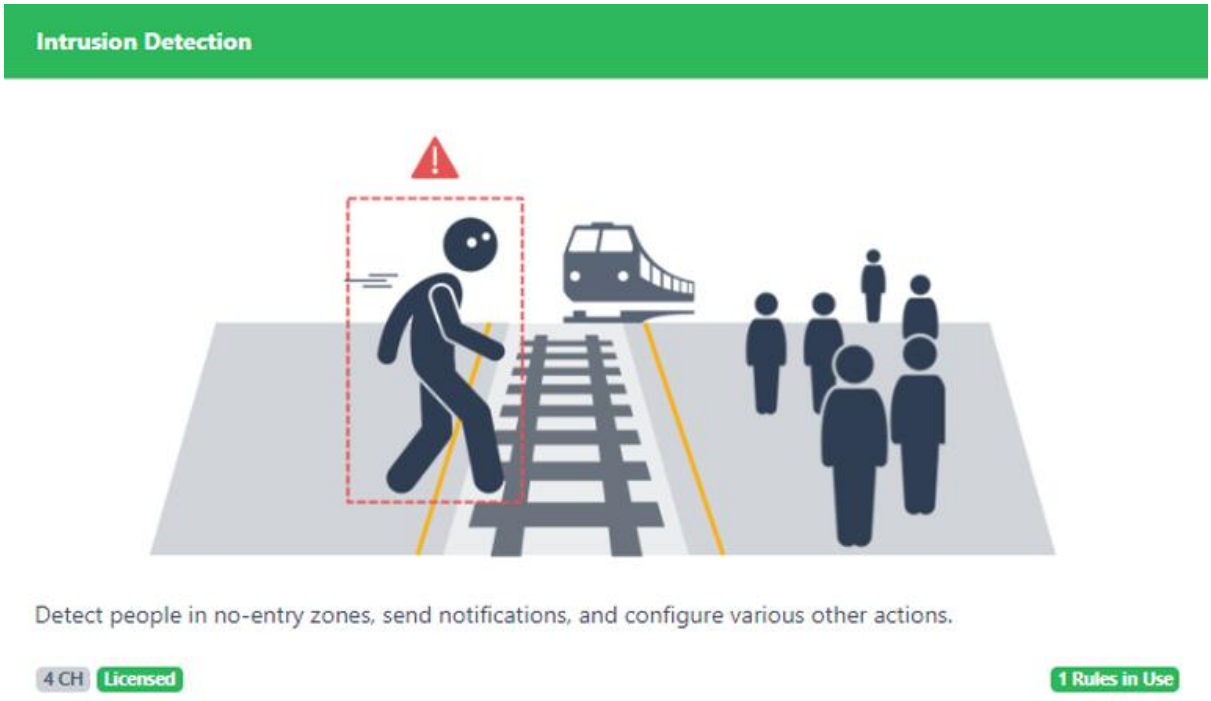
This is a section for creating AIBOX events.

Navigate to: APP SETTING > Explore AI Apps in the menu bar on the left.

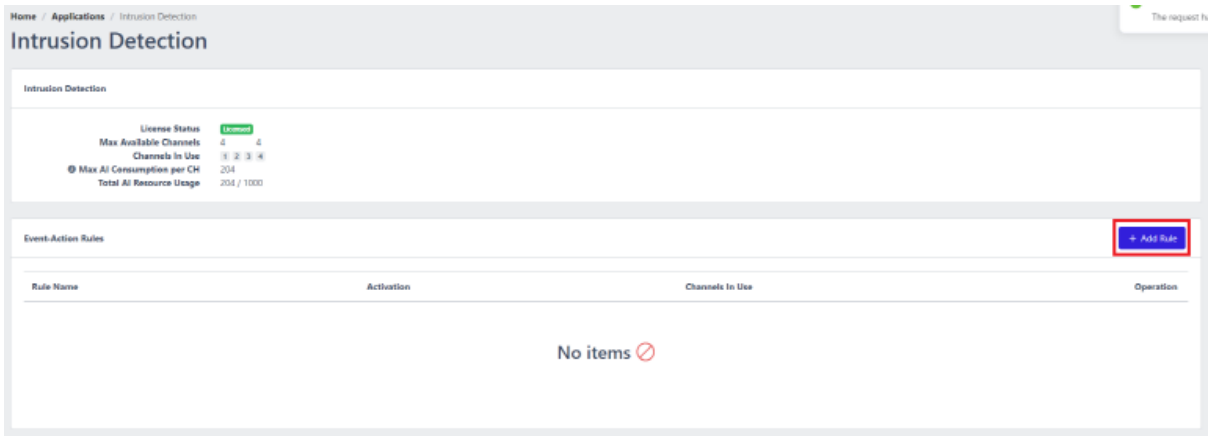


Select the desired AI feature from the available options.

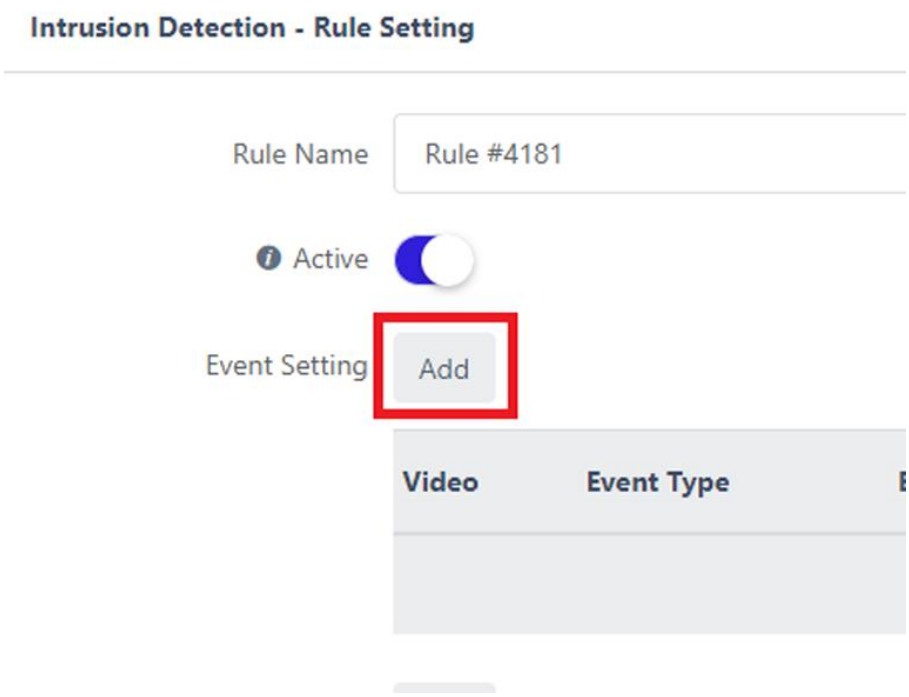
Note : As an example, Intrusion Detection.

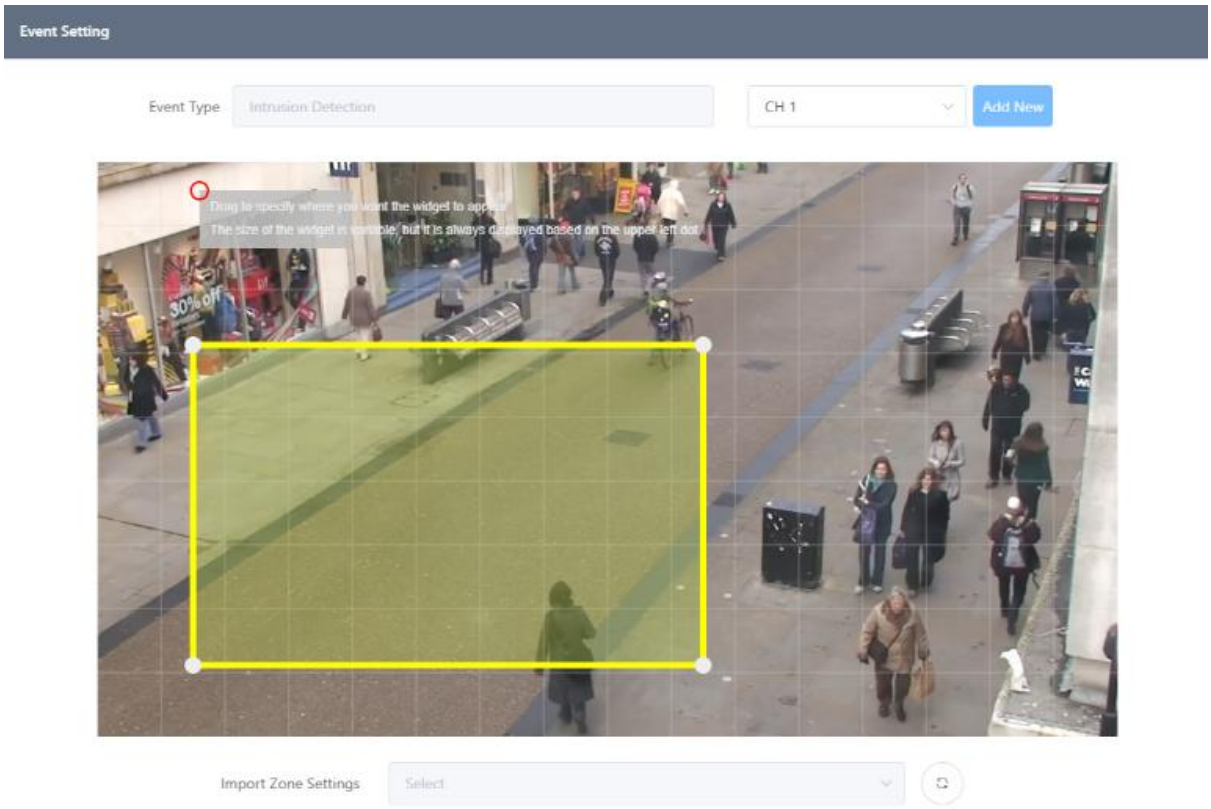


Click ‘Add Rule’.

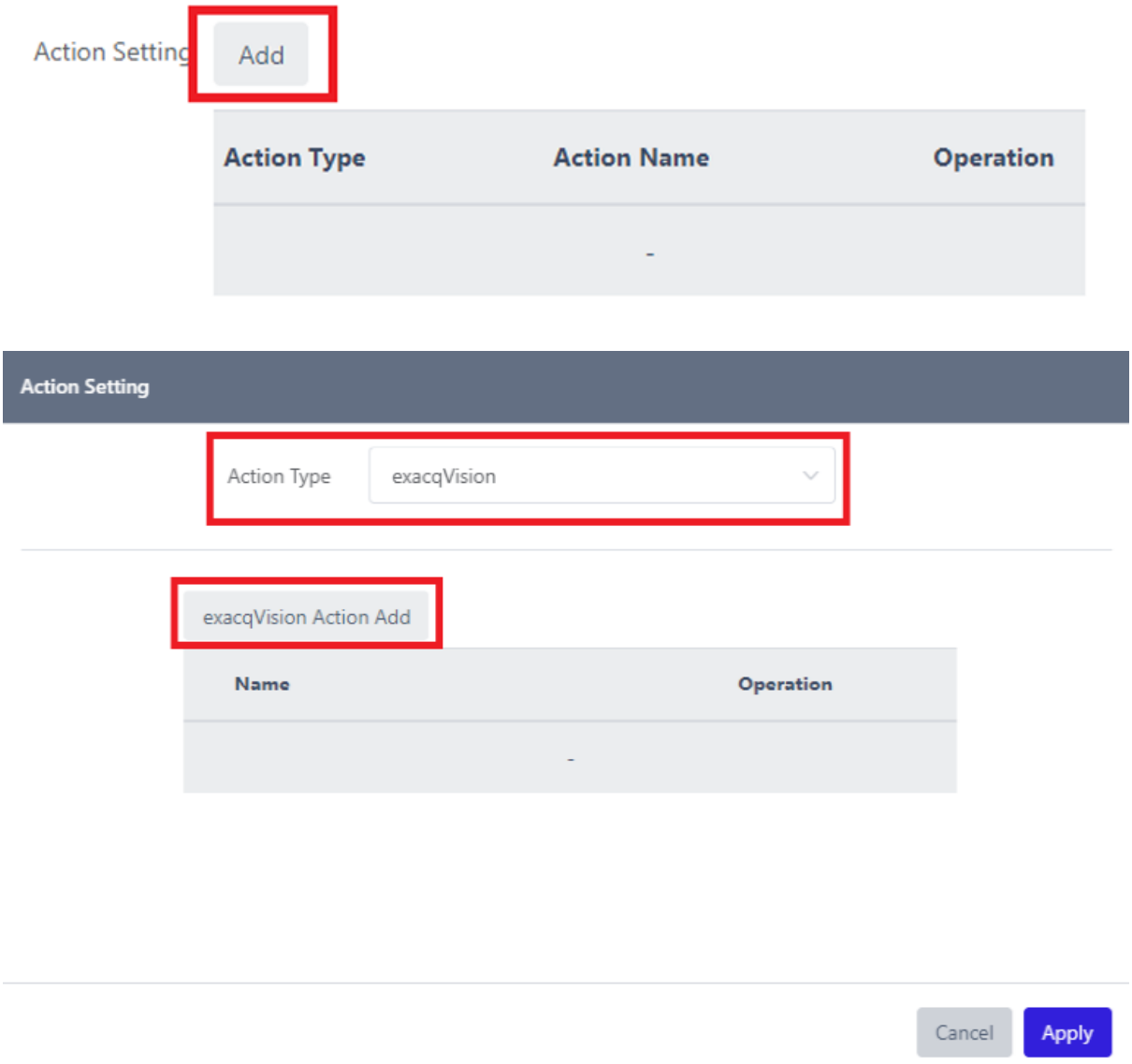


Add Event Setting, set the area, and click Apply.

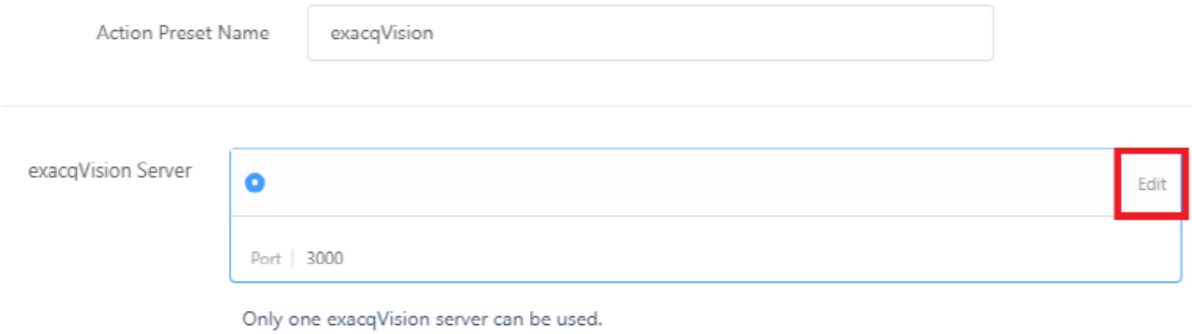




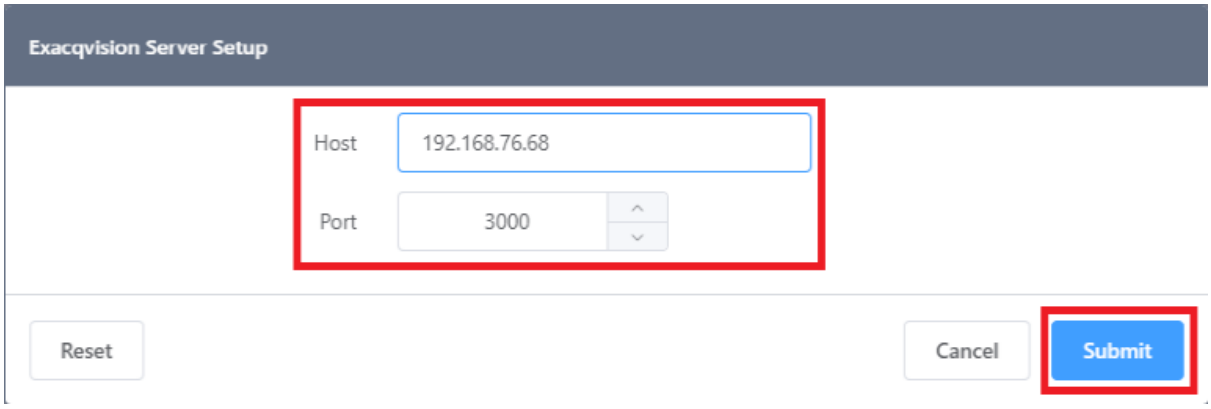
Add Action Setting, select exacqVision as the Action Type and check the box.



Modify exacqVision Server settings:

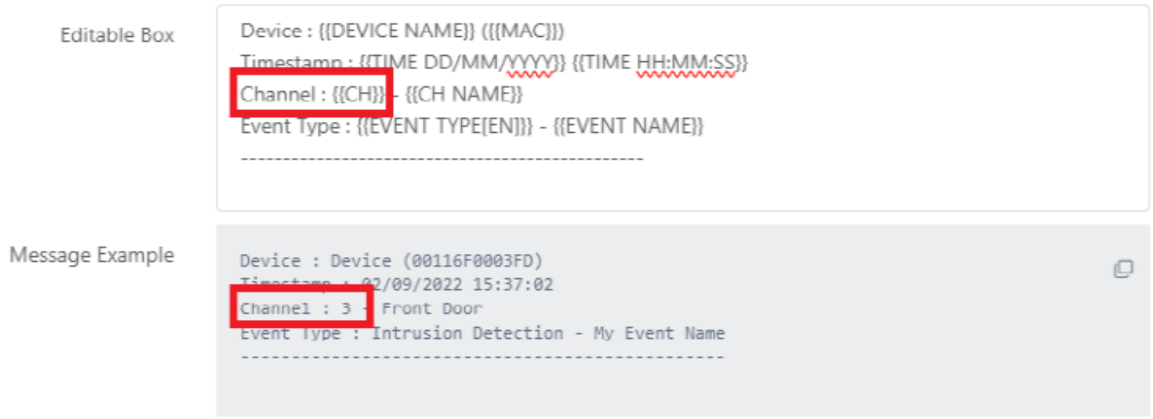


Enter the IP address of the exacqVision Server, and then enter the Port you created in Serial Ports in section 2.1.2.



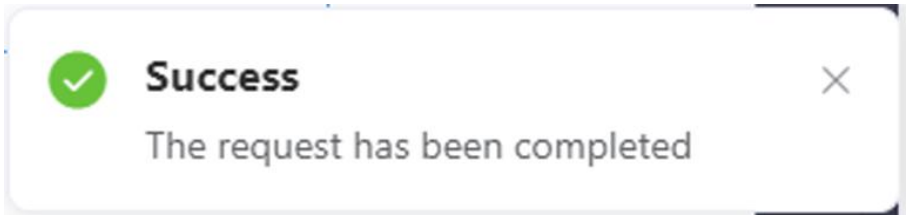
Fill in the Editable Box with the desired content. You can choose String Construction or use the desired Token values.

Note. To link Events to specific Channels in exacqVision, a field that distinguishes between channels must be present.

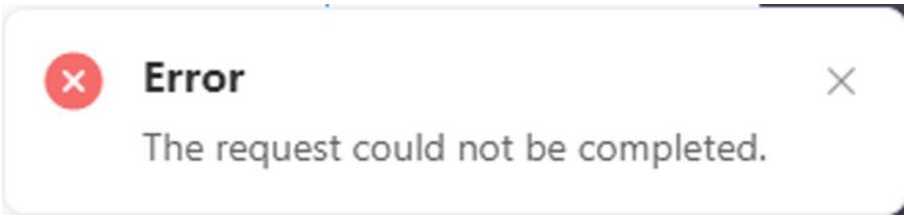


After filling in the message, click the Test button.

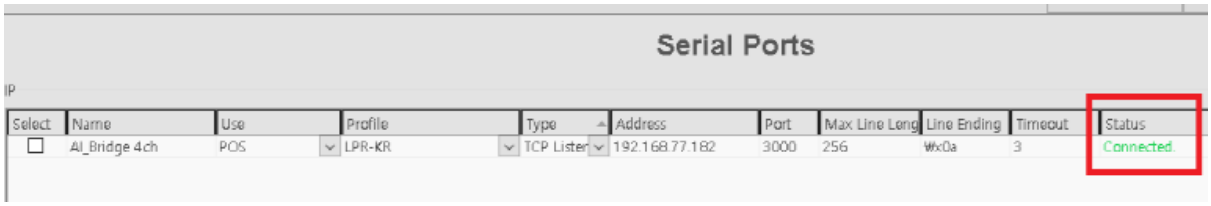
If the transmission is successful, a “Success” message will appear.

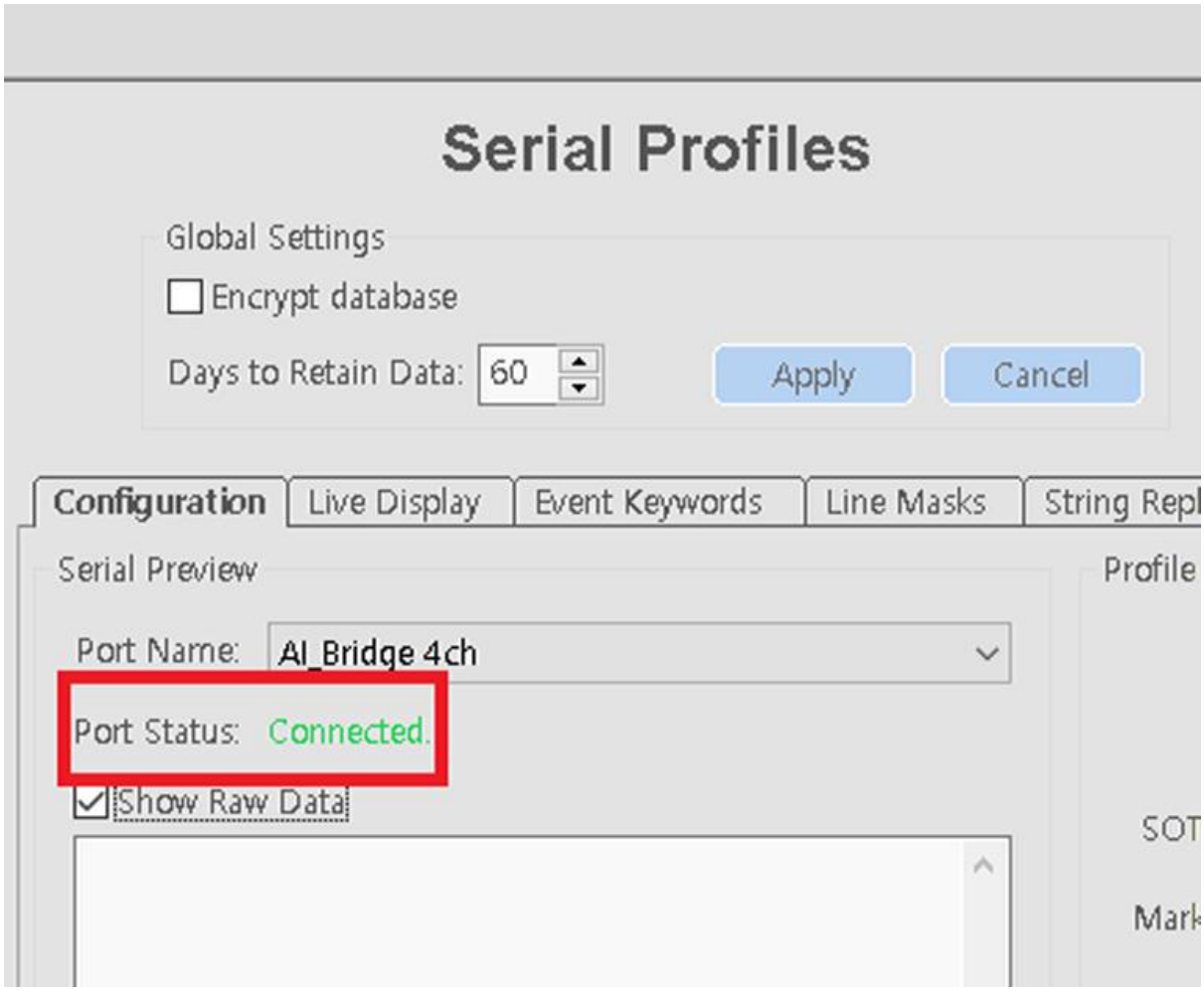


If the transmission fails, an “Error” message will appear. In this case, please check the server settings.



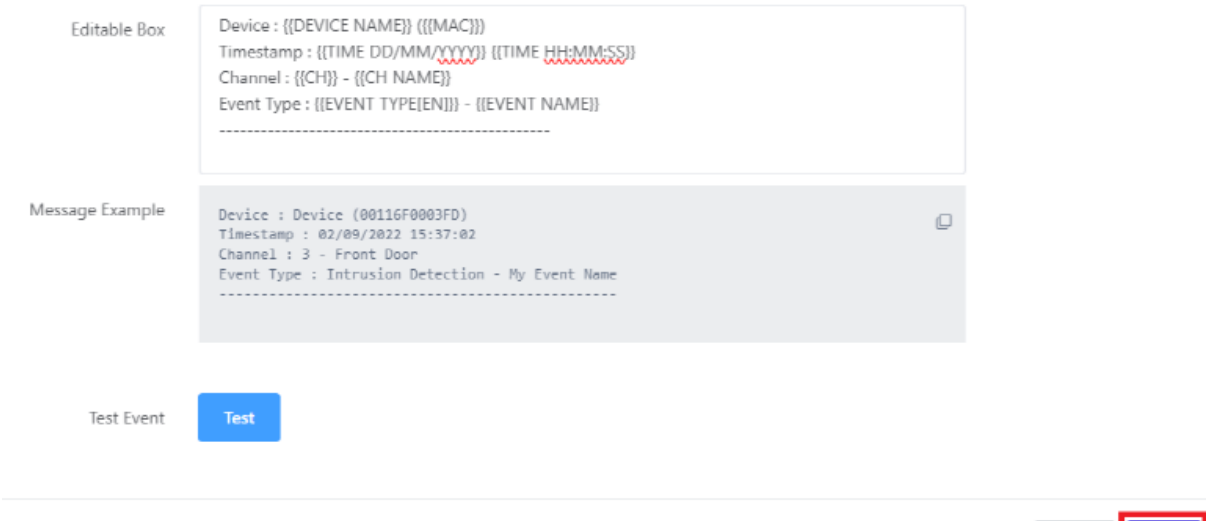
Note. There are two ways to check if the server is connected. You can verify the status in exacqVision by checking the Status in either the Serial Ports or Serial Profiles tabs.



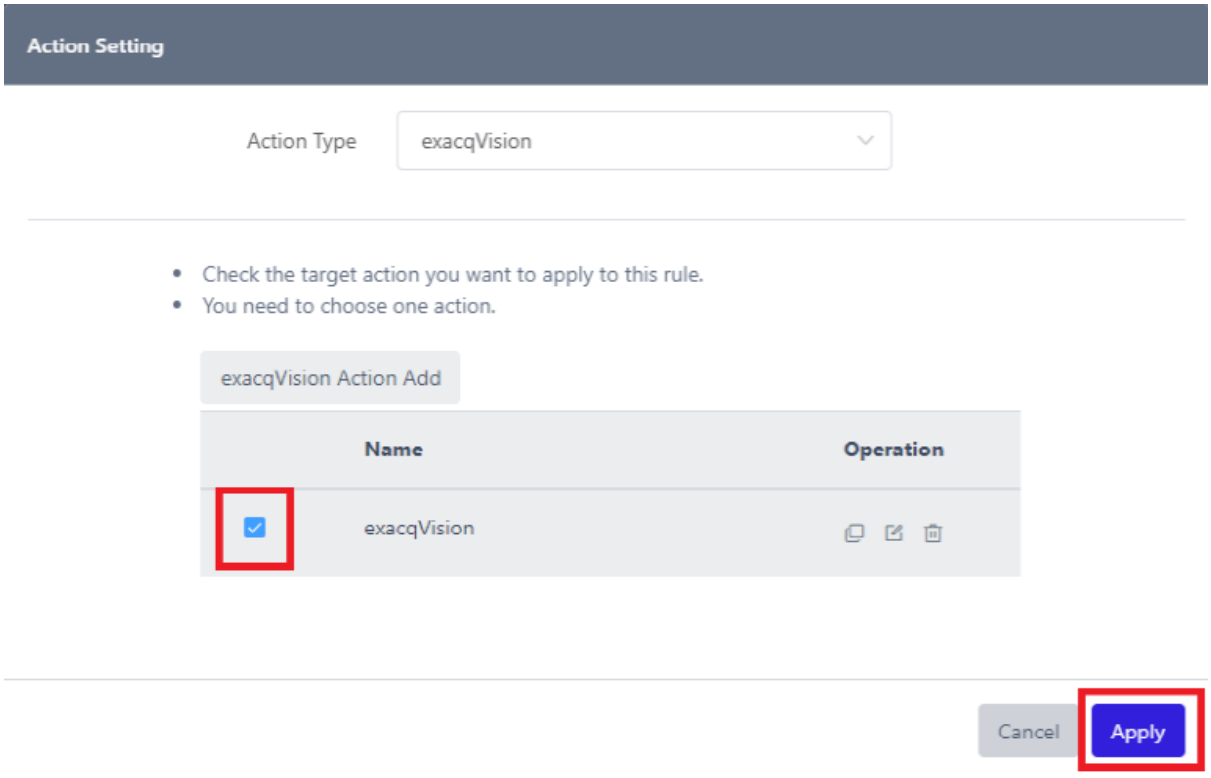


Note. If the event is not working properly, check the firewall
Note. How to Add a Rule or Port to a Windows 10 Firewall
https://www.youtube.com/watch?v=JsEulhg5P8k

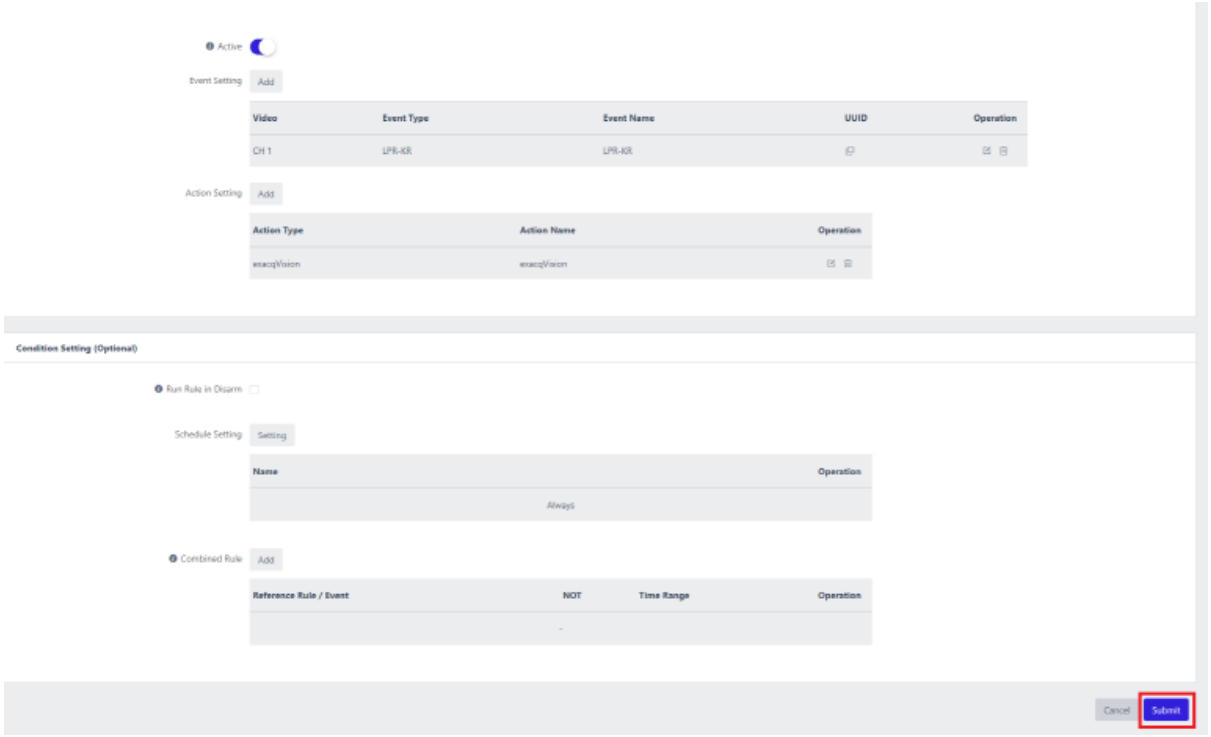
Once all settings are complete, click the Apply button.



Click on the exacqVision settings you created earlier, then click Apply.**Note.** If there are many detected objects and the message becomes too long, some objects may be truncated.



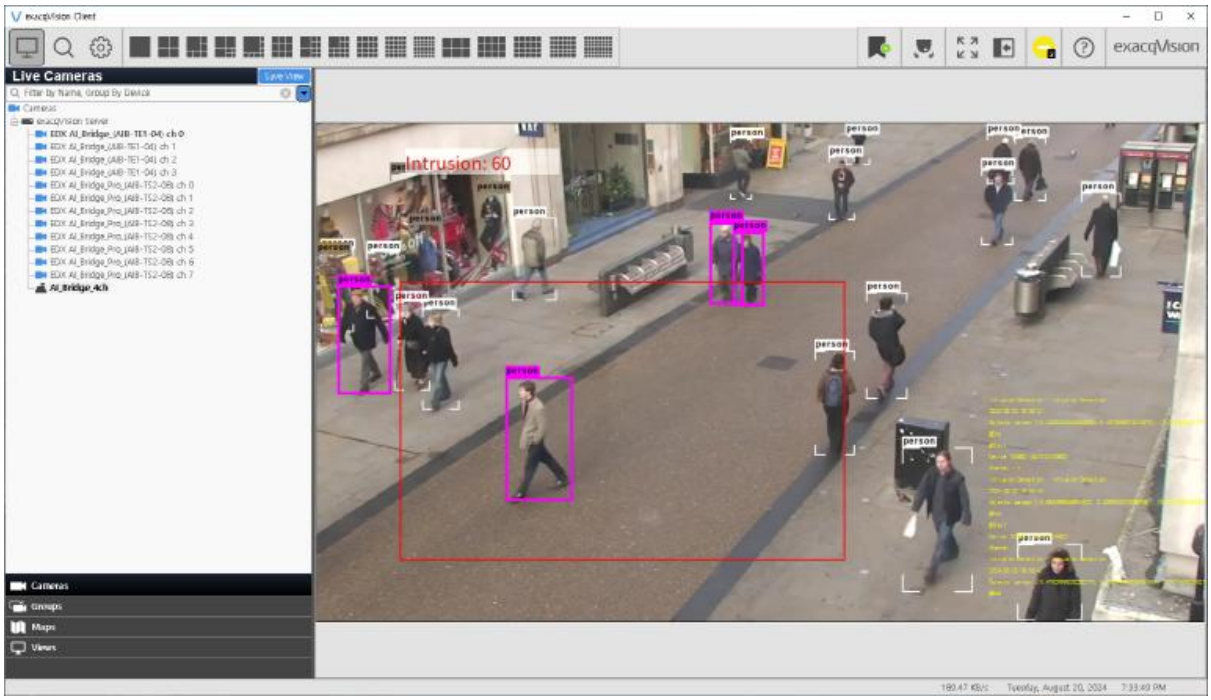
Finally, click the Submit button.



3. Demo

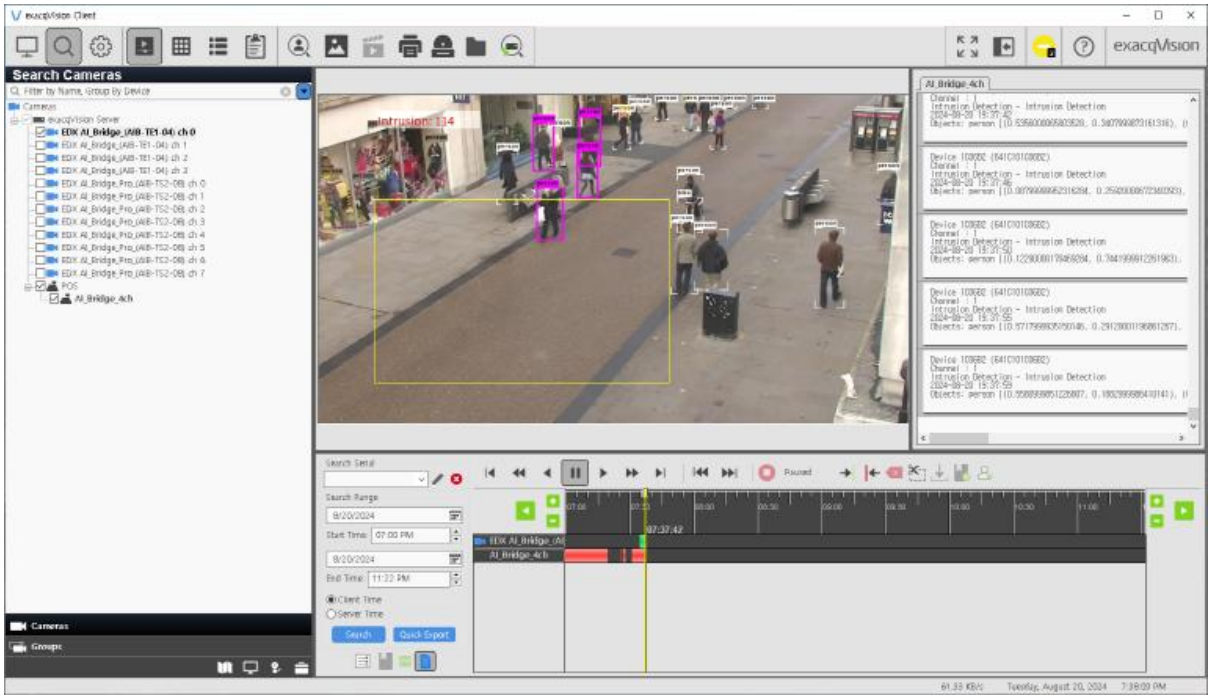
3.1 Live

In the Live Cameras tab of the exacqVision Client, you can check the Live Video.



3.2 Recording Search

TIP. If you select multiple videos, they will be displayed in a split-screen view.

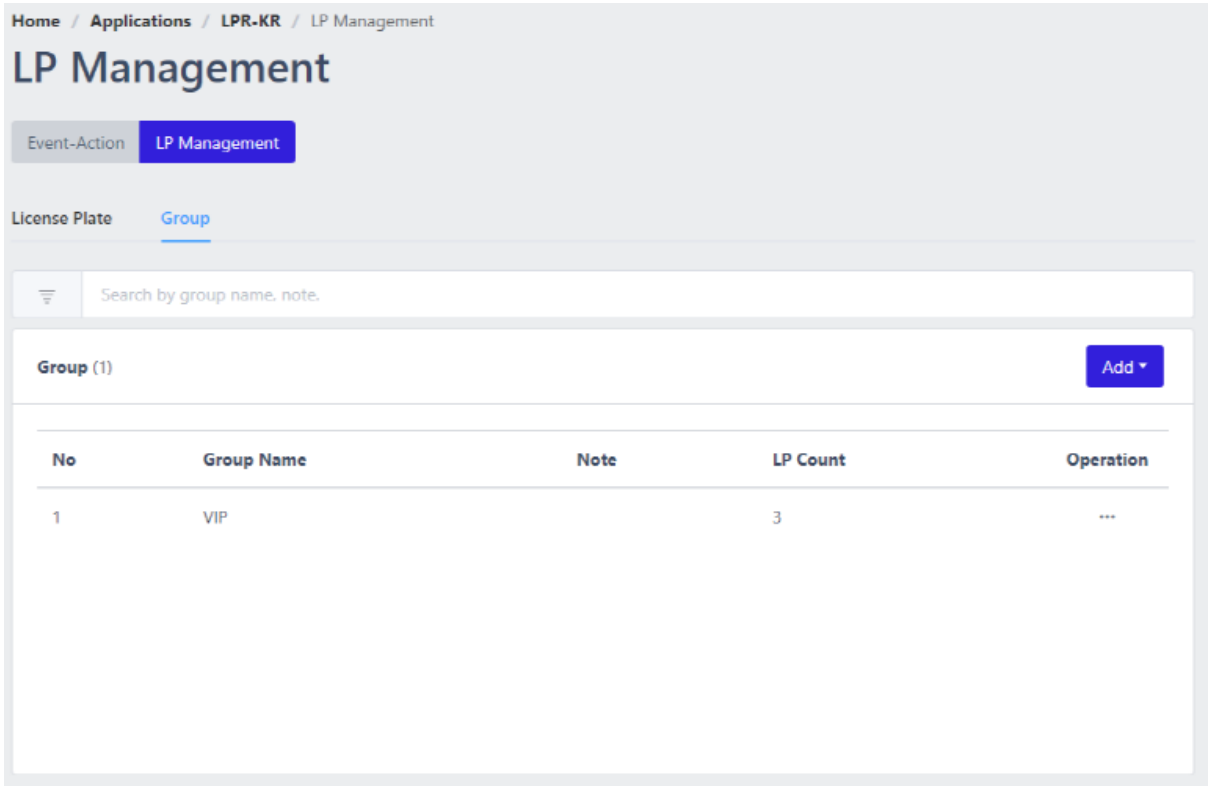


4. FAQ

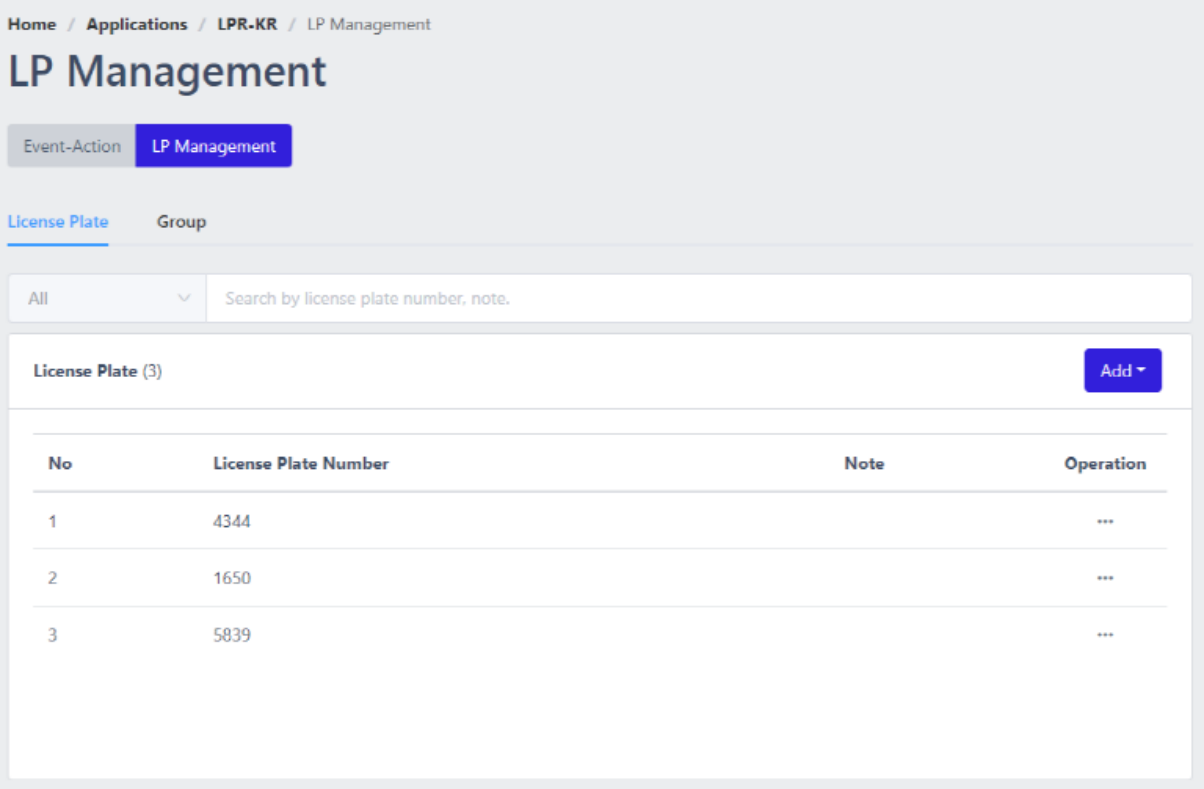
4.1 LPR Group scenario

As shown in the picture, using Group Mode in the LPR License allows for more efficient use of AI Events.

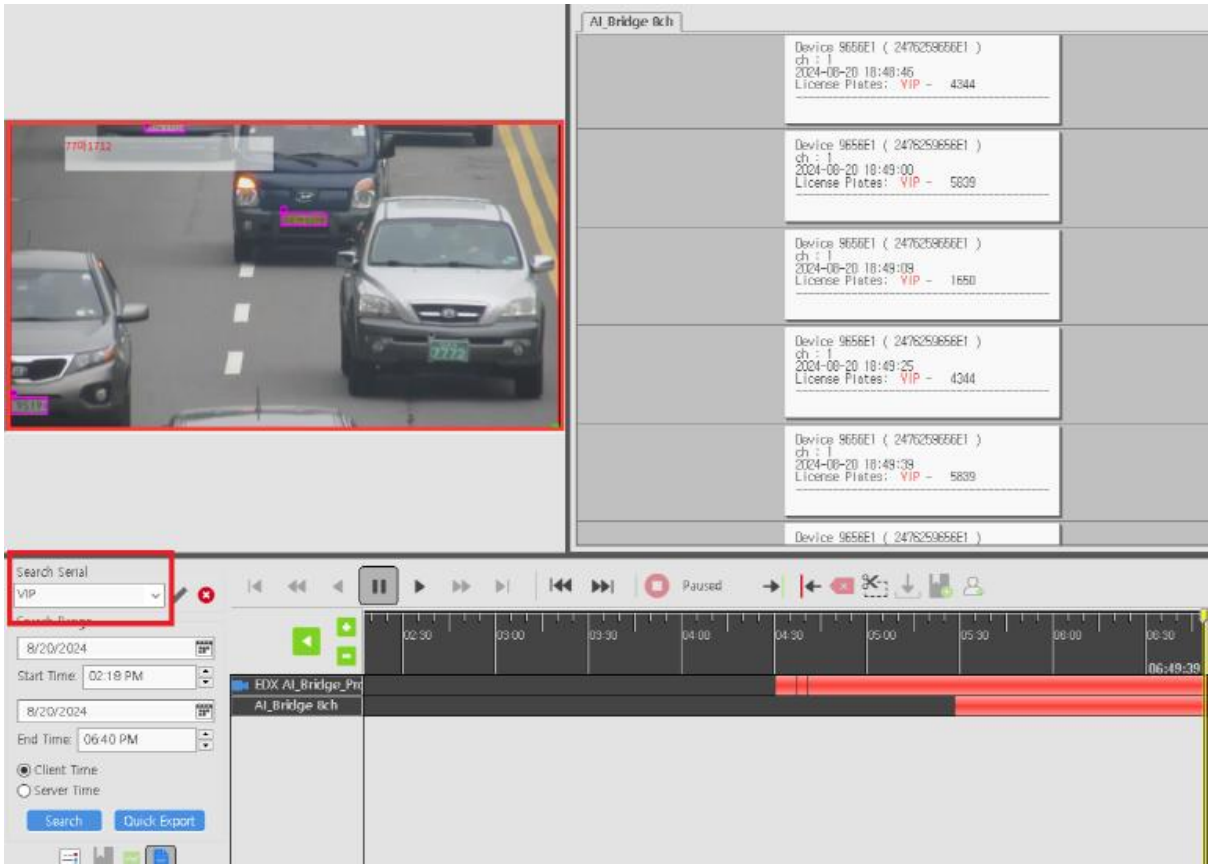
Add a Group.



Add the license plate number and select the Group..



When searching for VIP in Search Serial, it will appear as shown below.



Make sure that **LP_GROUP_NAME** is included in the Editable Box

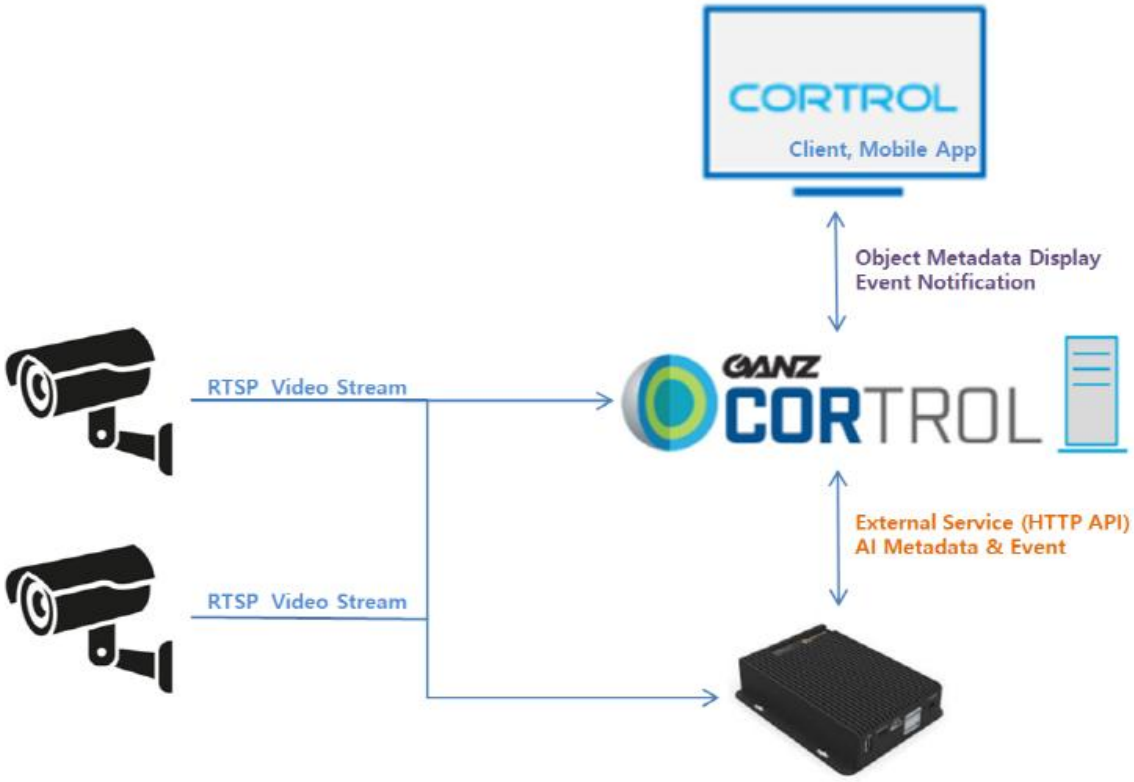
Ganz Cortrol Integration Guide

1. Introduction

1.1 Prerequisites

- AIBOX FW version 10124 or greater.
- Ganz Cortrol Premier/ Global VMS version 1.22 or greater.

1.2 Learn about integration architecture



IP Camera transmits video stream to Cortrol VMS and AIBOX.

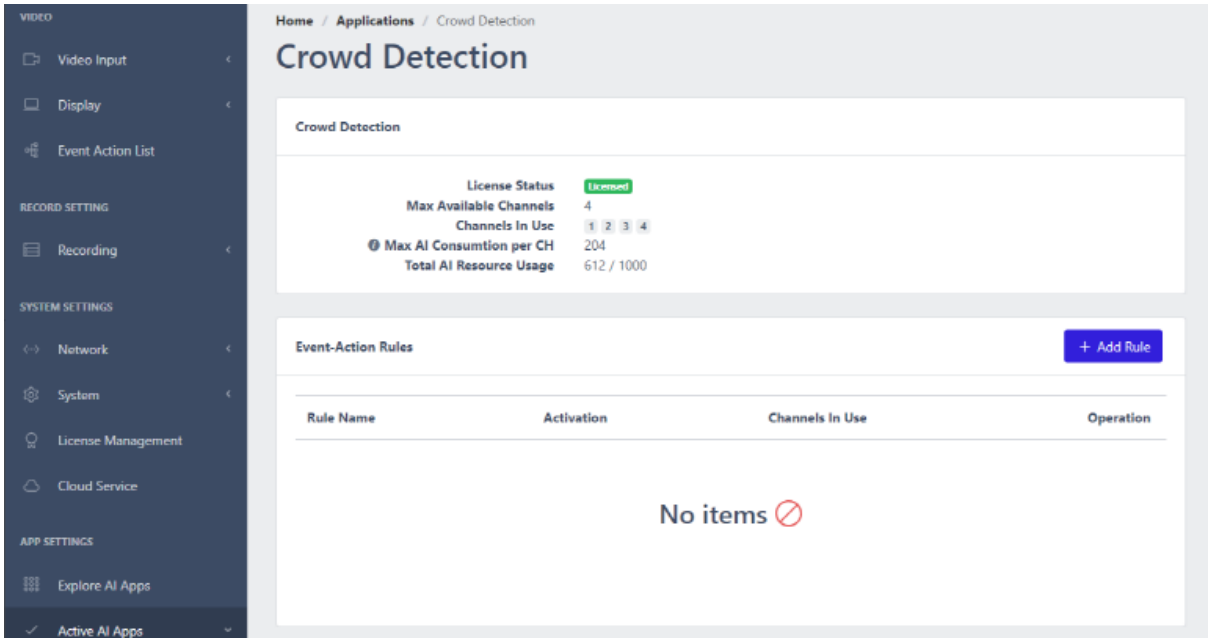
AIBOX analyzes the received video stream by AI Apps and sends metadata & event to Cortrol VMS.

AIBOX responds to Cortrol VMS's search requests.

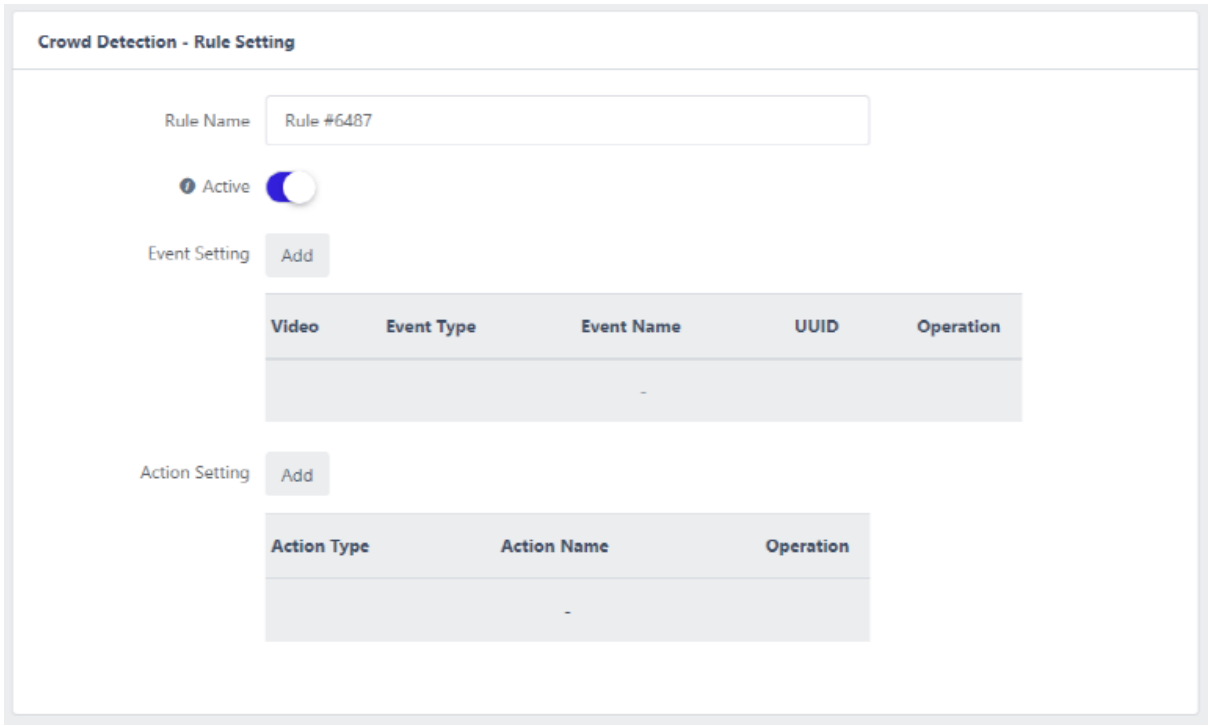
2. Configuration

2.1 AIBOX Configuration

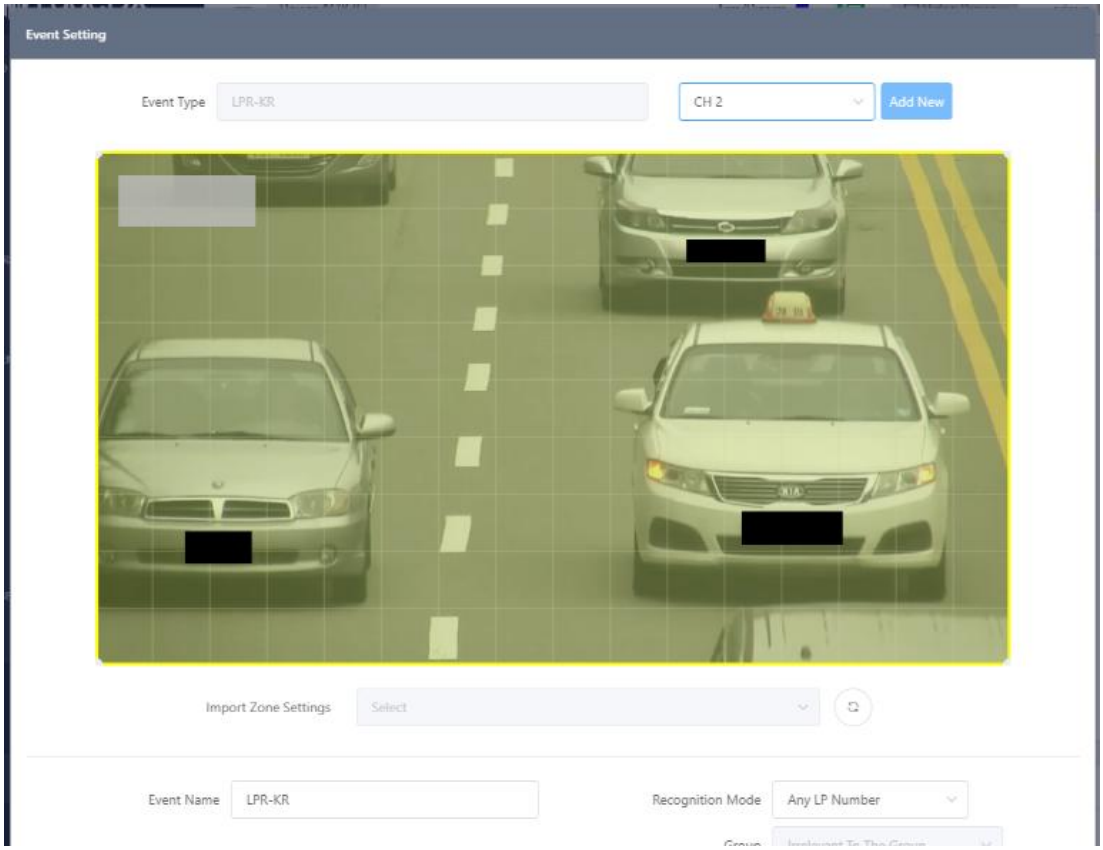
Add AI app settings.



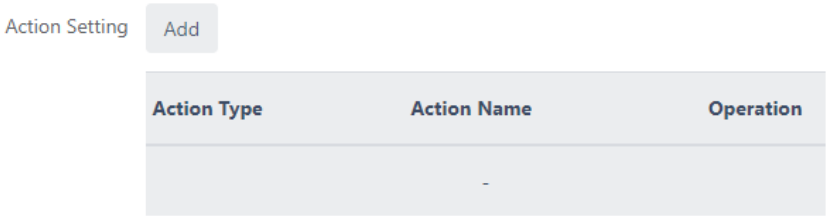
Add Event Setting.



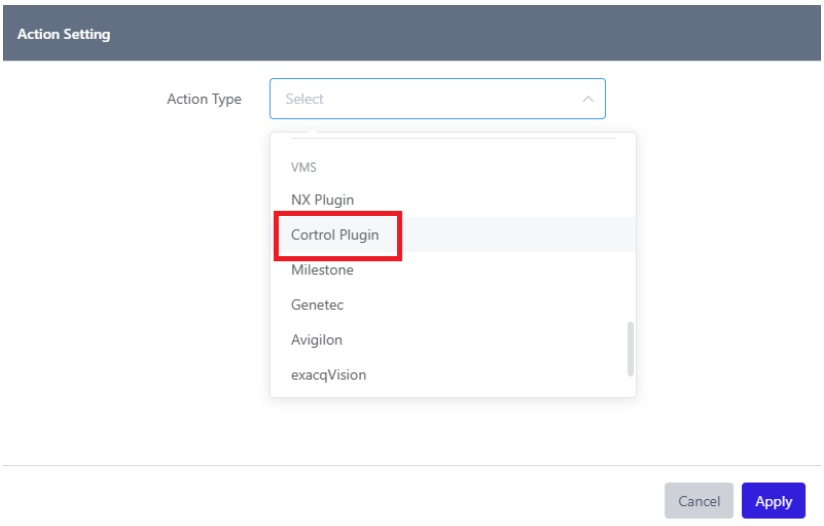
Zone or detailed setting of AI App.



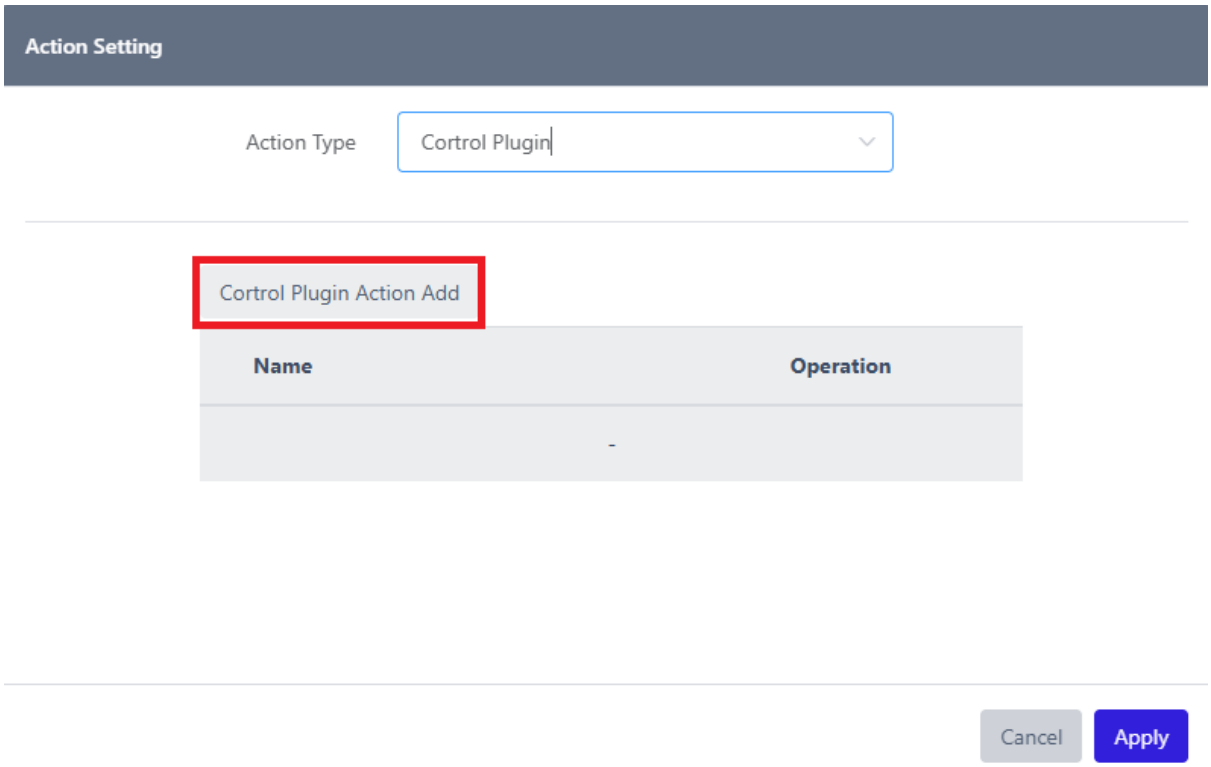
Add Cortrol Plugin Action Setting.



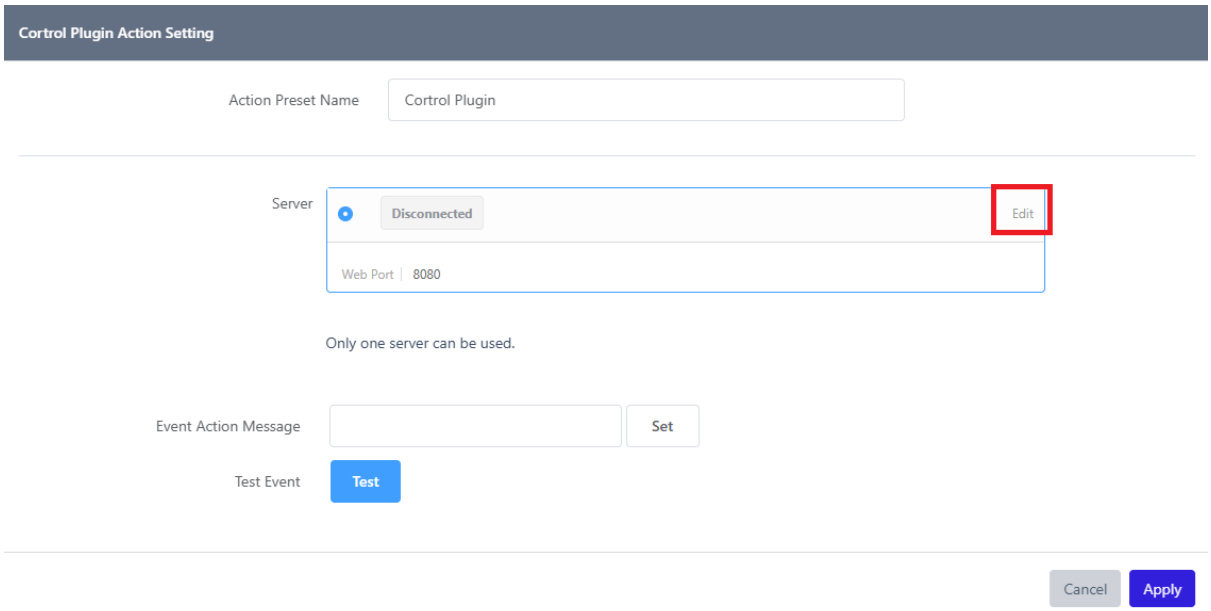
Select Cortrol Plugin.



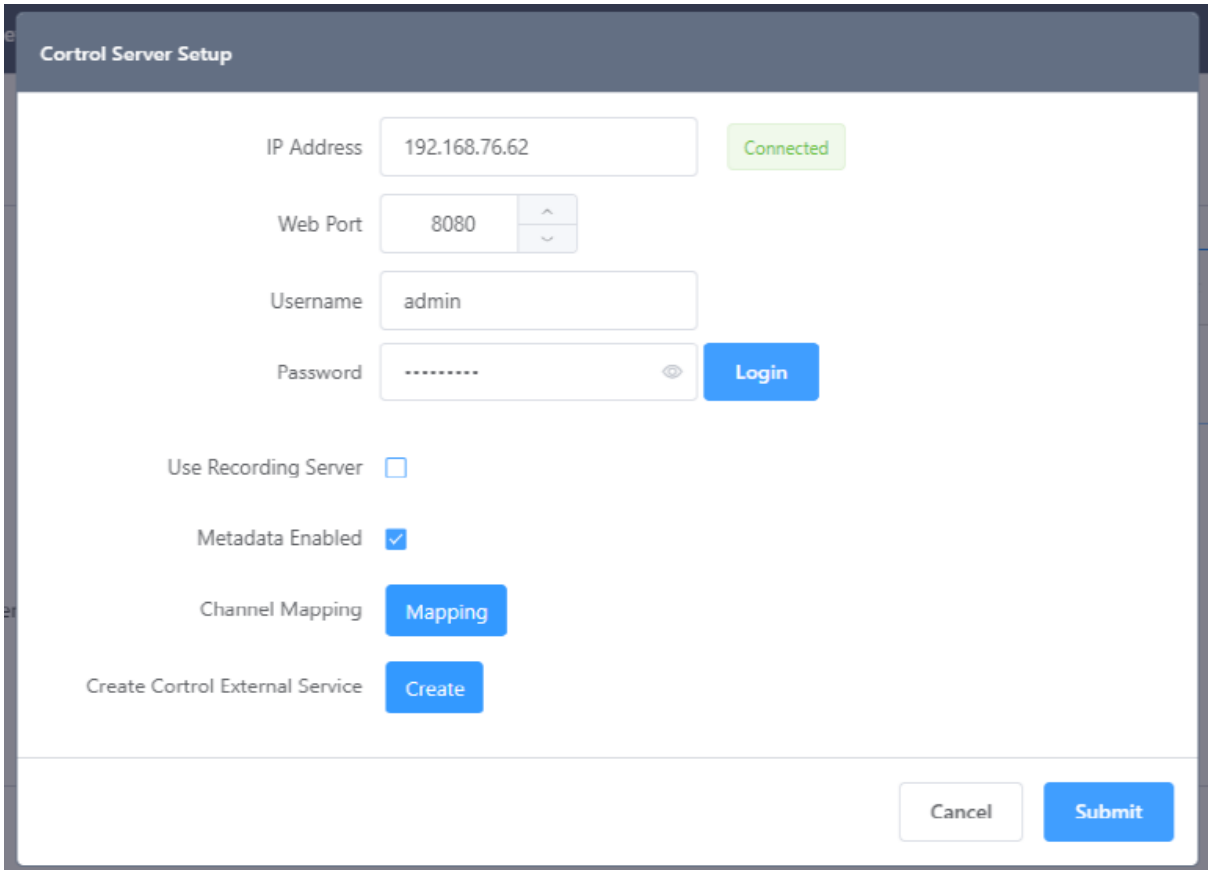
Click the “Cortrol Plugin Action Add” button.

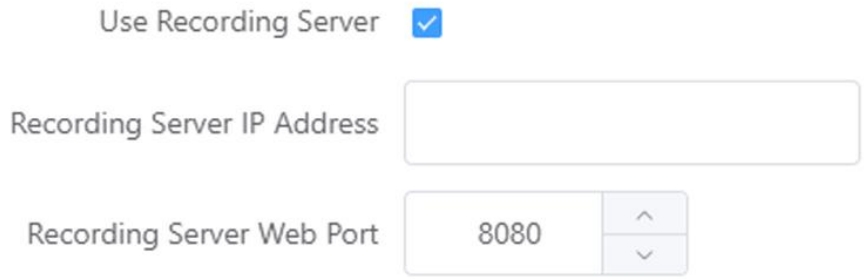


Click the “Edit” button.



Enter the Cortrol VMS information (Server Address, Port number, Username, Password)
You can check if the Cortrol VMS settings are correct through the **“Login”** button.





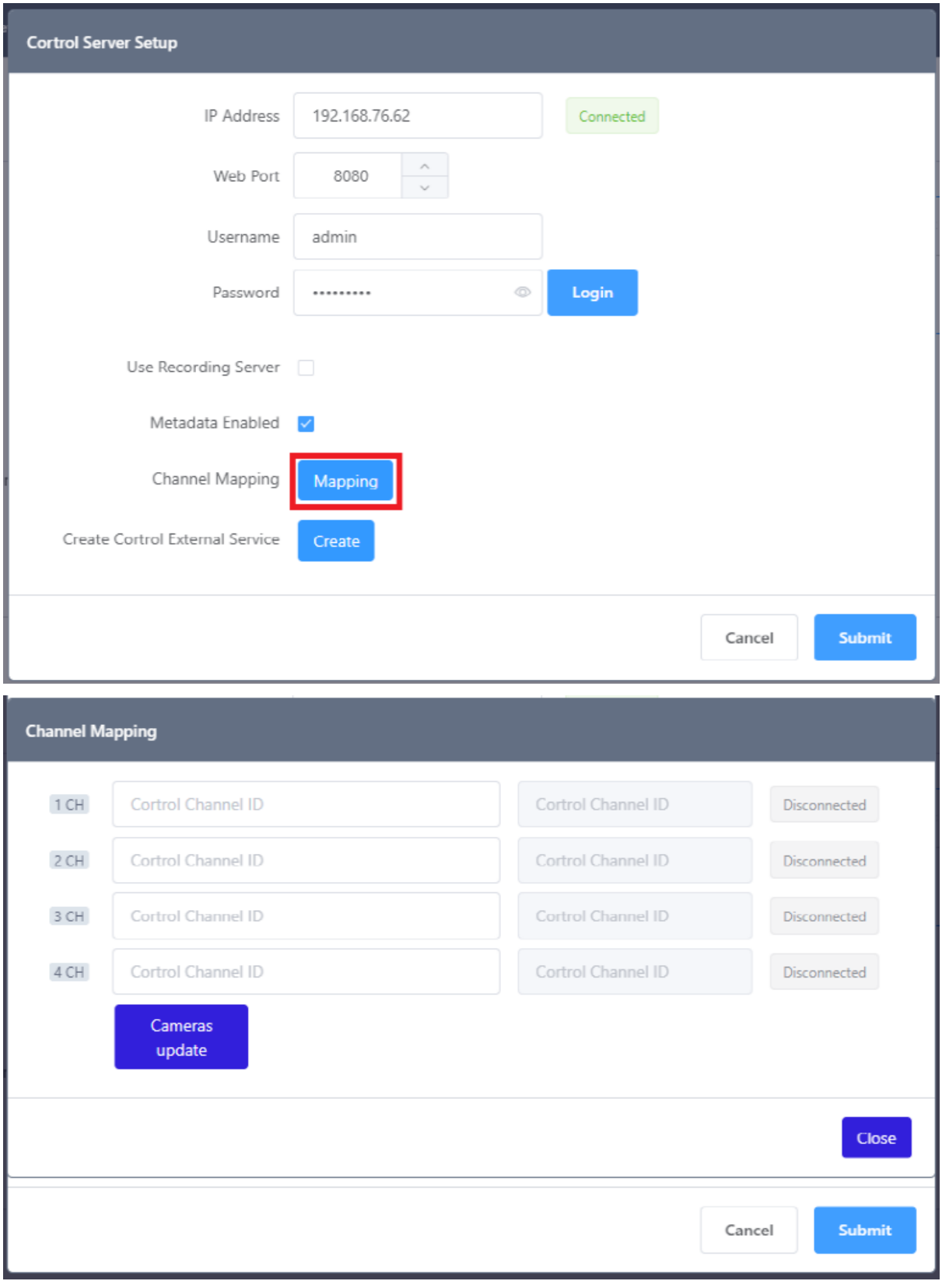
Note. When **"Metadata Enable"** is enabled, AIBOX transmits object Metadata detected by AI to Control VMS. Please note that performance issues may occur if the AI app is installed in an environment where many objects are detected.

Note. If you are a Cortrol Global user and have registered the device using Cortrol Recording, please check 'Use Recording Server and enter the ID and password. For the Cortrol Premier version, you do not need to check this option.

2.2 AIBOX Channel Mapping

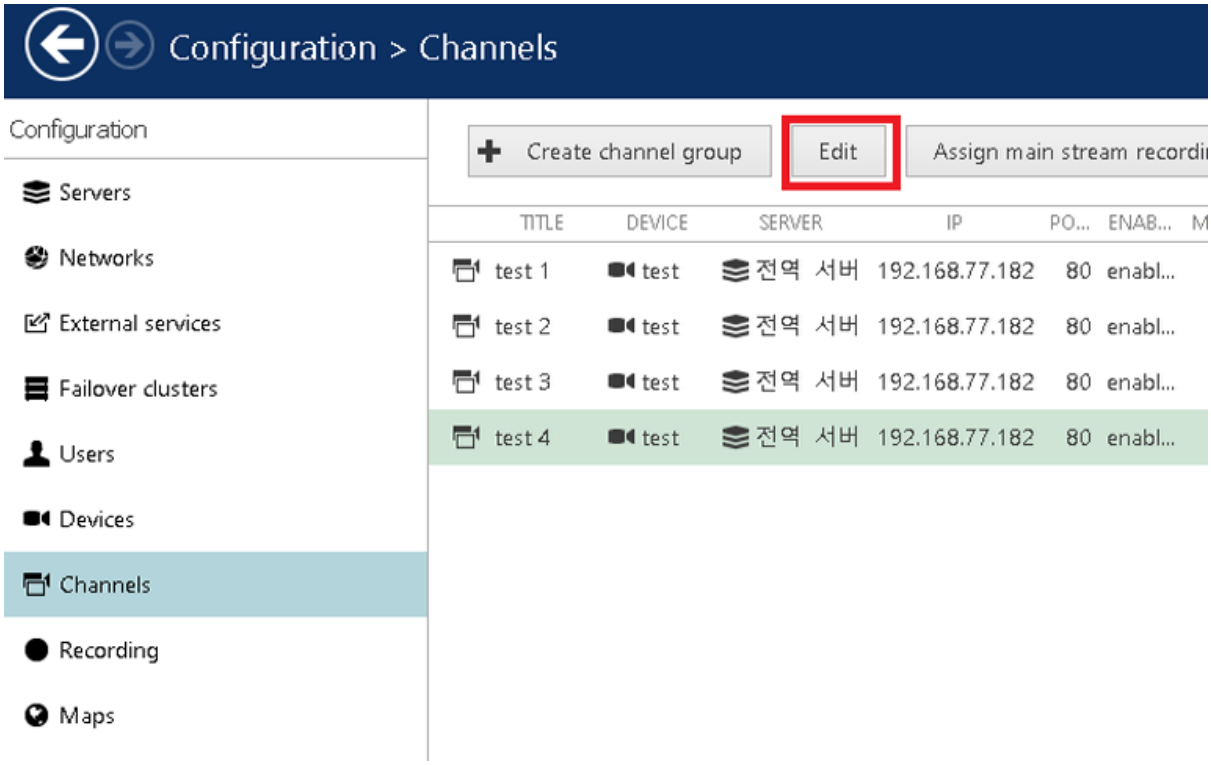
Set up the relationship between the AIBOX channel and the channel of Cortrol VMS.

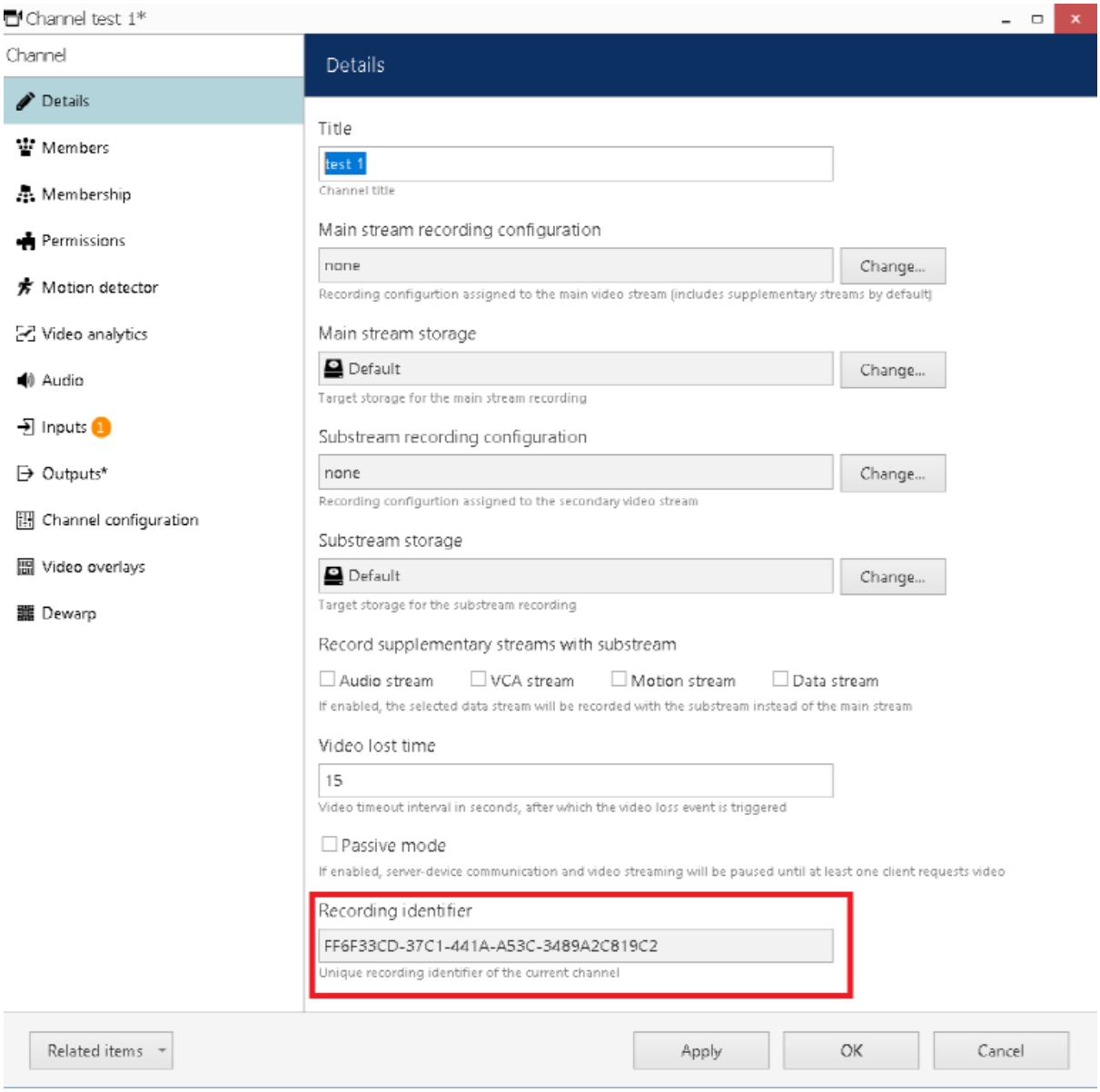
Press the "Mapping" button to open the settings pop-up window.

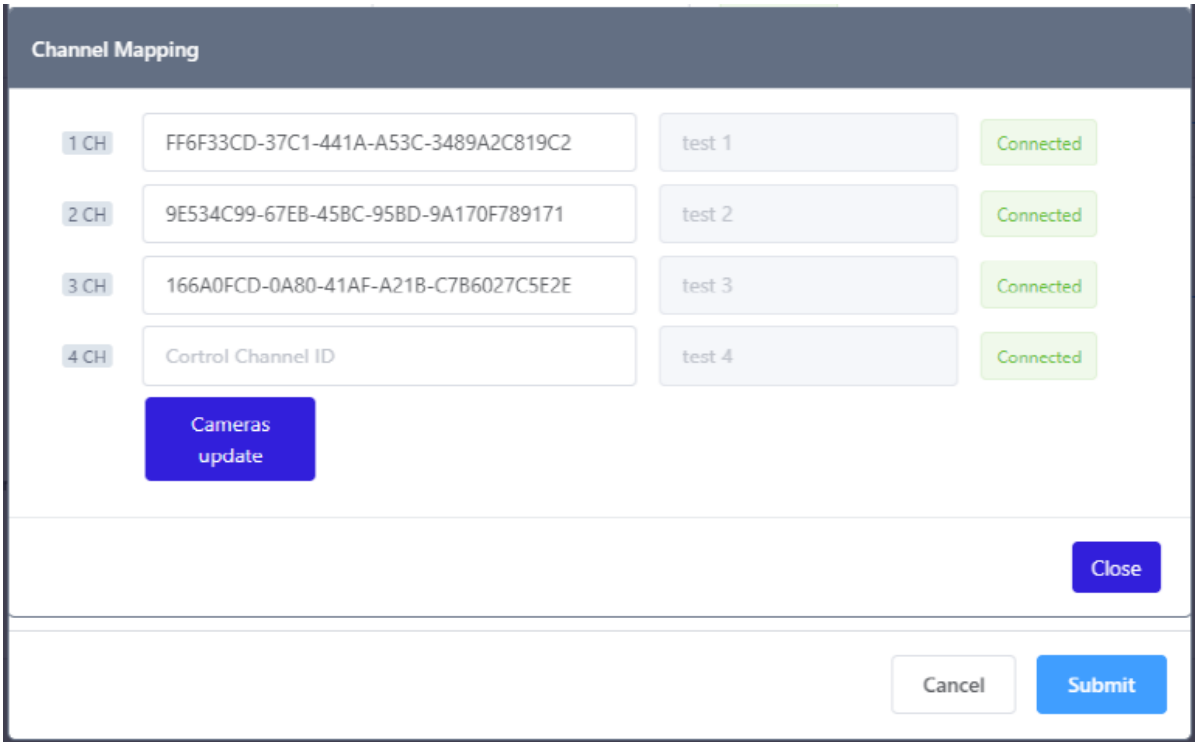


Enter the **Recording identifier (UUID)** of the channel registered in Control VMS into AIBOX.

Recording identifier (UUID) can be obtained from the Details menu of Channel in Control Management Console.


Configuration > Channels
Configuration
Servers
Networks
External services
Failover clusters
Users
Devices
Channels
Recording
Maps
Create channel group
Edit
Assign main stream recordi
TITLE
DEVICE
SERVER
IP
PO...
ENAB...
M
test 1
test
전역 서버
192.168.77.182
80
enabl...
test 2
test
전역 서버
192.168.77.182
80
enabl...
test 3
test
전역 서버
192.168.77.182
80
enabl...
test 4
test
전역 서버
192.168.77.182
80
enabl...

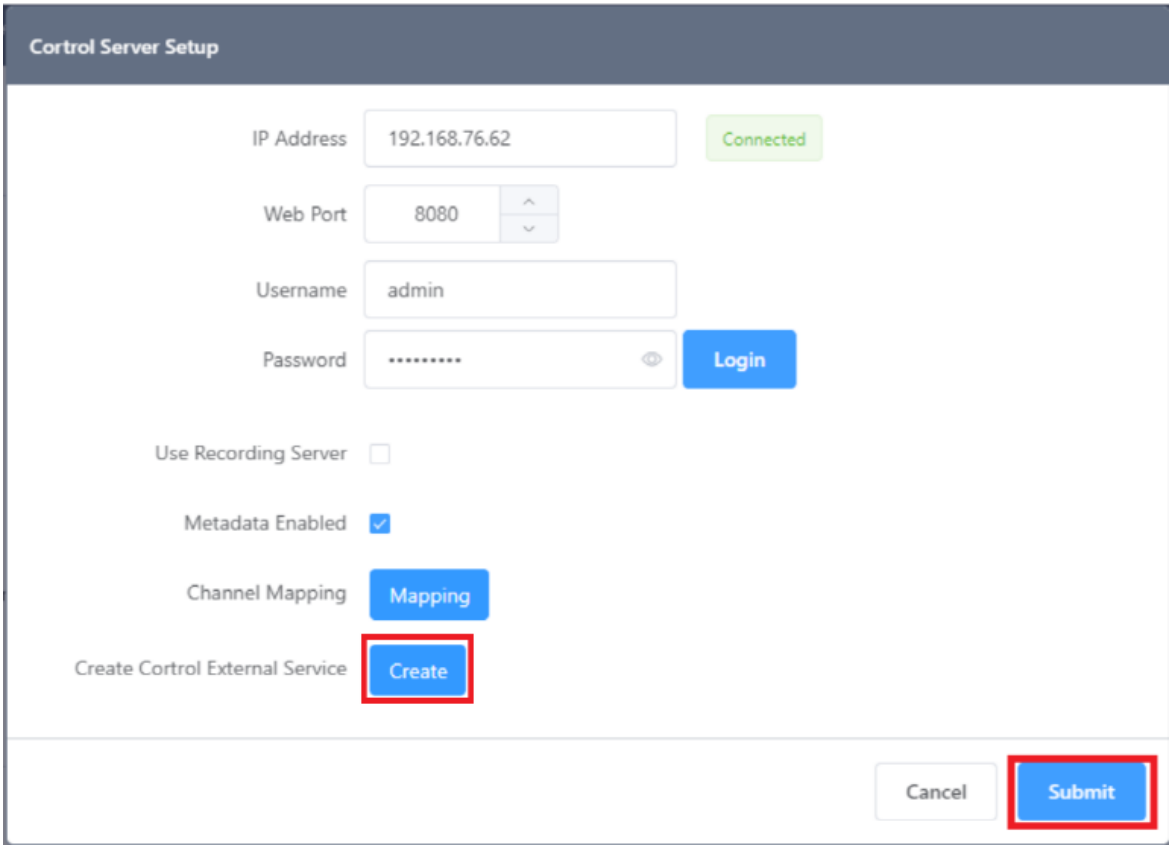

Channel test 1*
Channel
Details
Members
Membership
Permissions
Motion detector
Video analytics
Audio
Inputs 1
Outputs*
Channel configuration
Video overlays
Dewarp
Details
Title
test 1
Channel title
Main stream recording configuration
none
Change...
Recording configurtion assigned to the main video stream (includes supplementary streams by default)
Main stream storage
Default
Change...
Target storage for the main stream recording
Substream recording configuration
none
Change...
Recording configurtion assigned to the secondary video stream
Substream storage
Default
Change...
Target storage for the substream recording
Record supplementary streams with substream
Audio stream
VCA stream
Motion stream
Data stream
If enabled, the selected data stream will be recorded with the substream instead of the main stream
Video lost time
15
Video timeout interval in seconds, after which the video loss event is triggered
Passive mode
If enabled, server-device communication and video streaming will be paused until at least one client requests video
Recording identifier
FF6F33CD-37C1-441A-A53C-3489A2C819C2
Unique recording identifier of the current channel
Related items
Apply
OK
Cancel



Enter the **Recording identifier (UUID)** and press the **"Cameras update"** button to check if it is entered correctly. If the channel is connected successfully, green Connected is displayed.

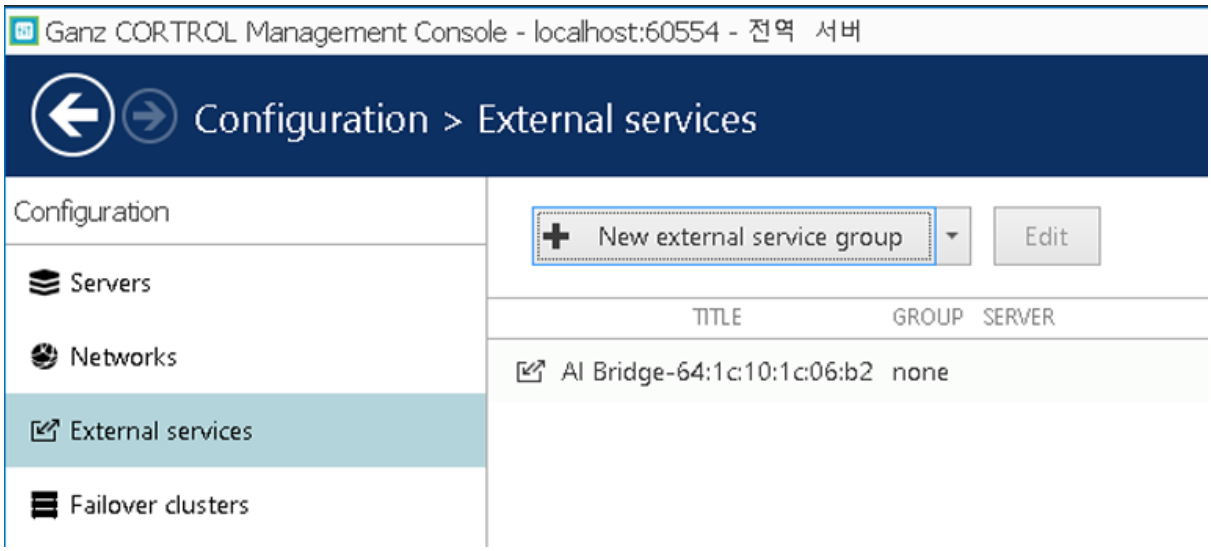
2.3 Create Control External Service

Create an external service by clicking the **"Create"** button on AIBOX's "Control VMS Setup page".

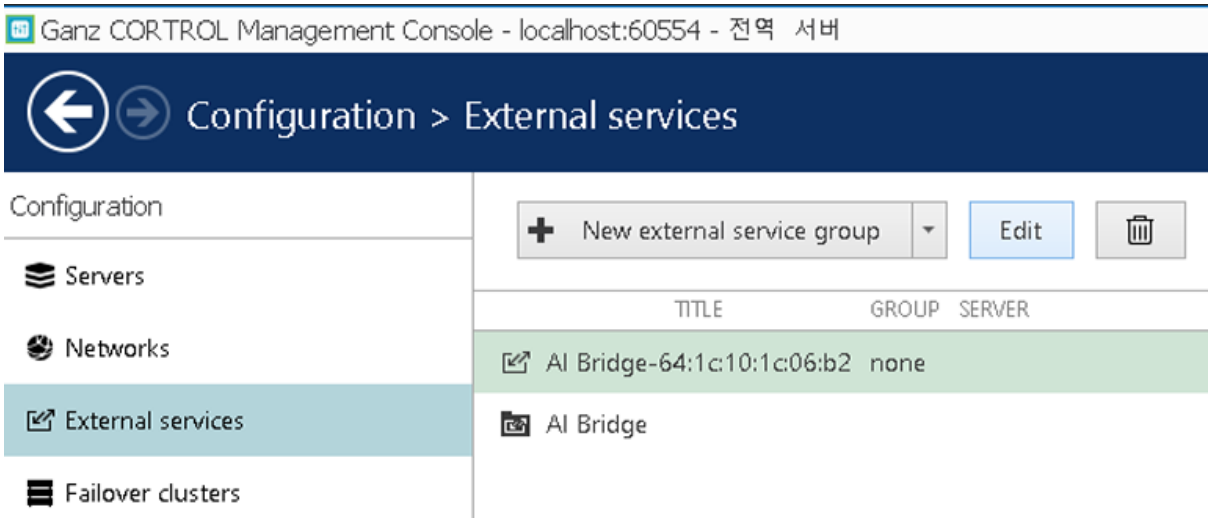


Note. Clicking Create will reset the Group mapping, so you will need to map it again. Rule settings and other configurations will not be reset.

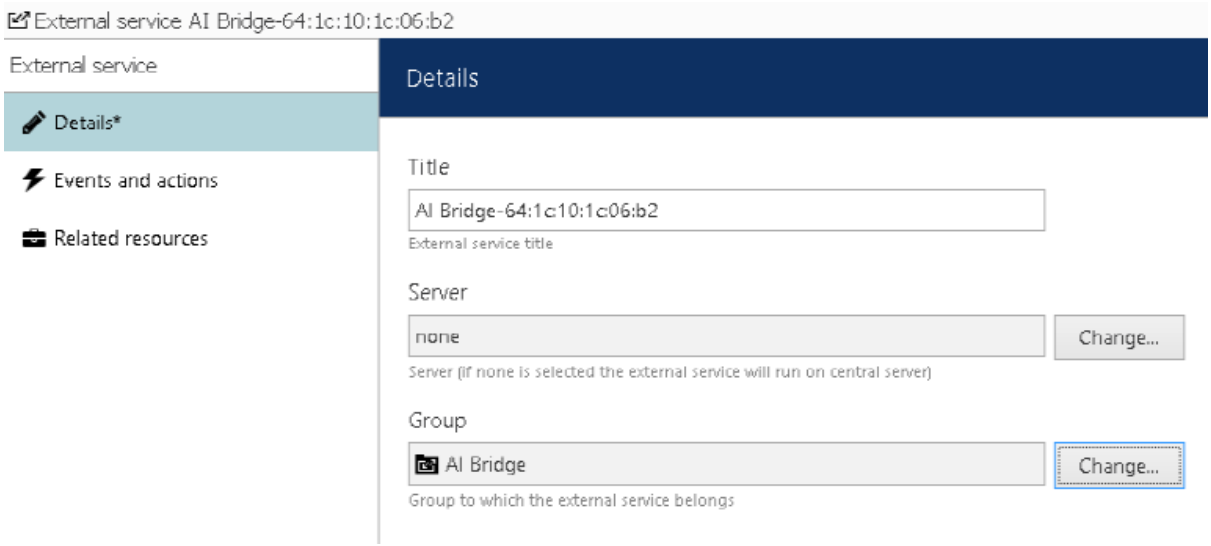
Next, Create an External Service Group.



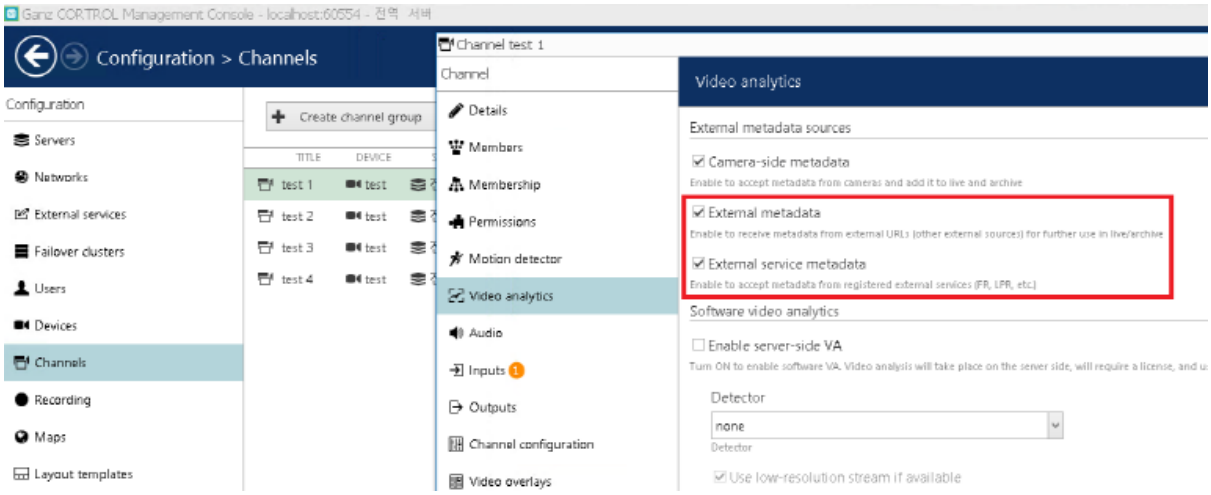
Enter the name of the new External Service Group as **“AIBOX”**.



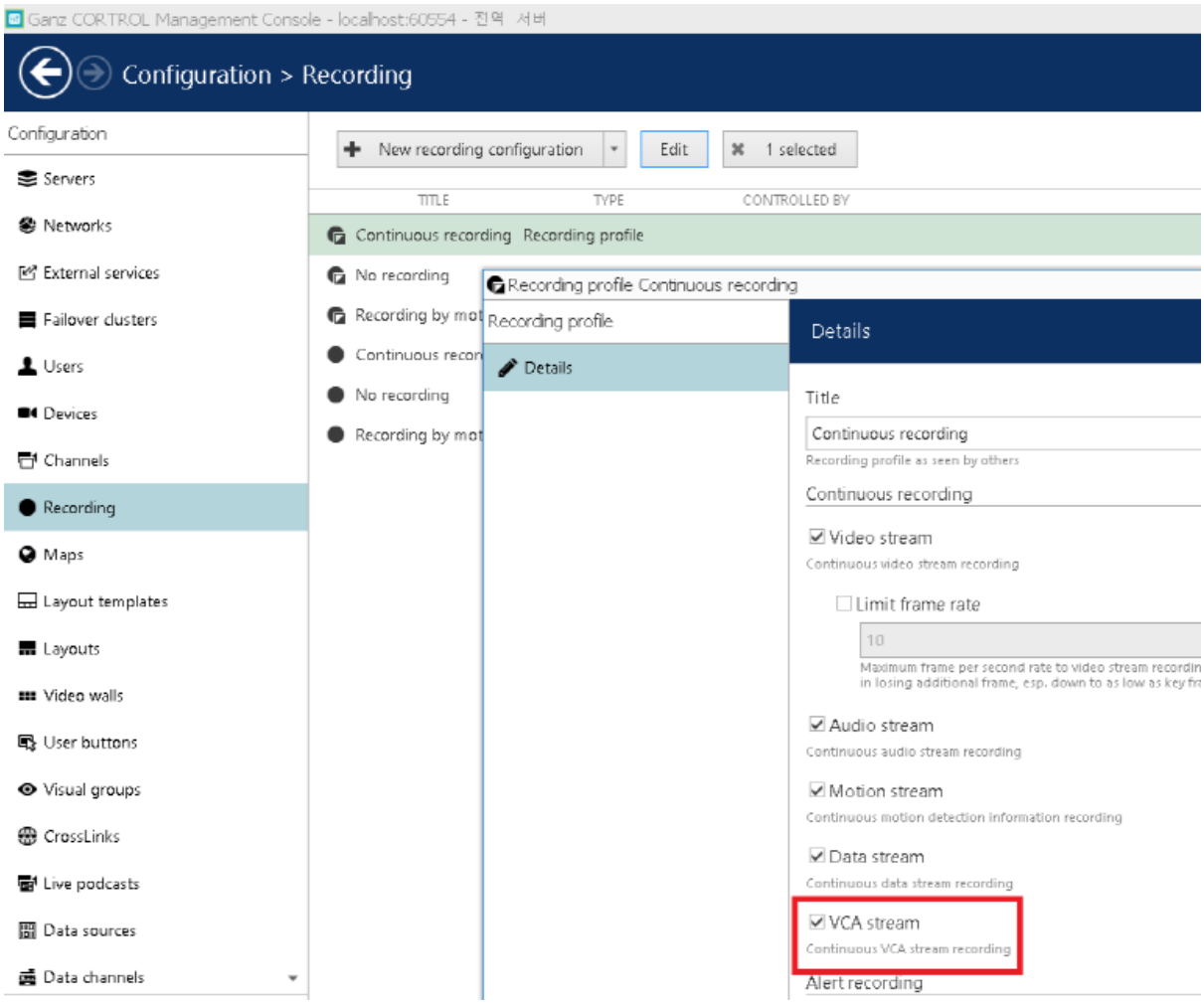
Assign AIBOX to the new External Service Group.



Note. If you are using the Cortrol Recording Server, please select the Cortrol Recording Server in the Server settings.



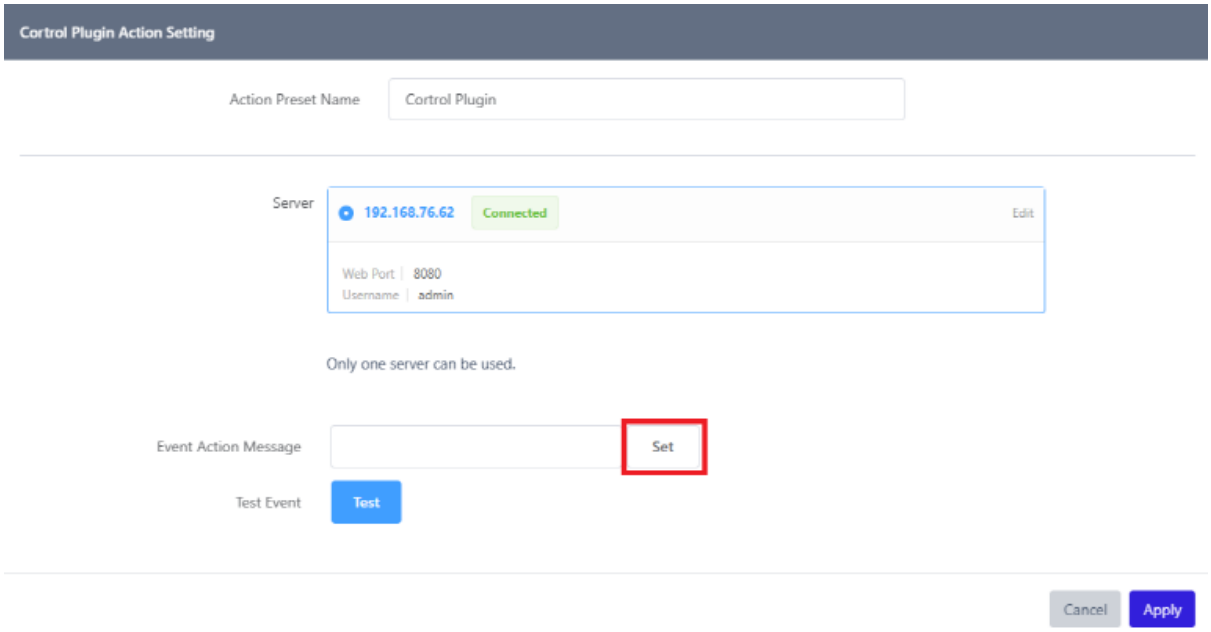
Note. To use the external service, you need to enable the external usage settings in every channel configuration. You need to configure this setting separately for each channel.



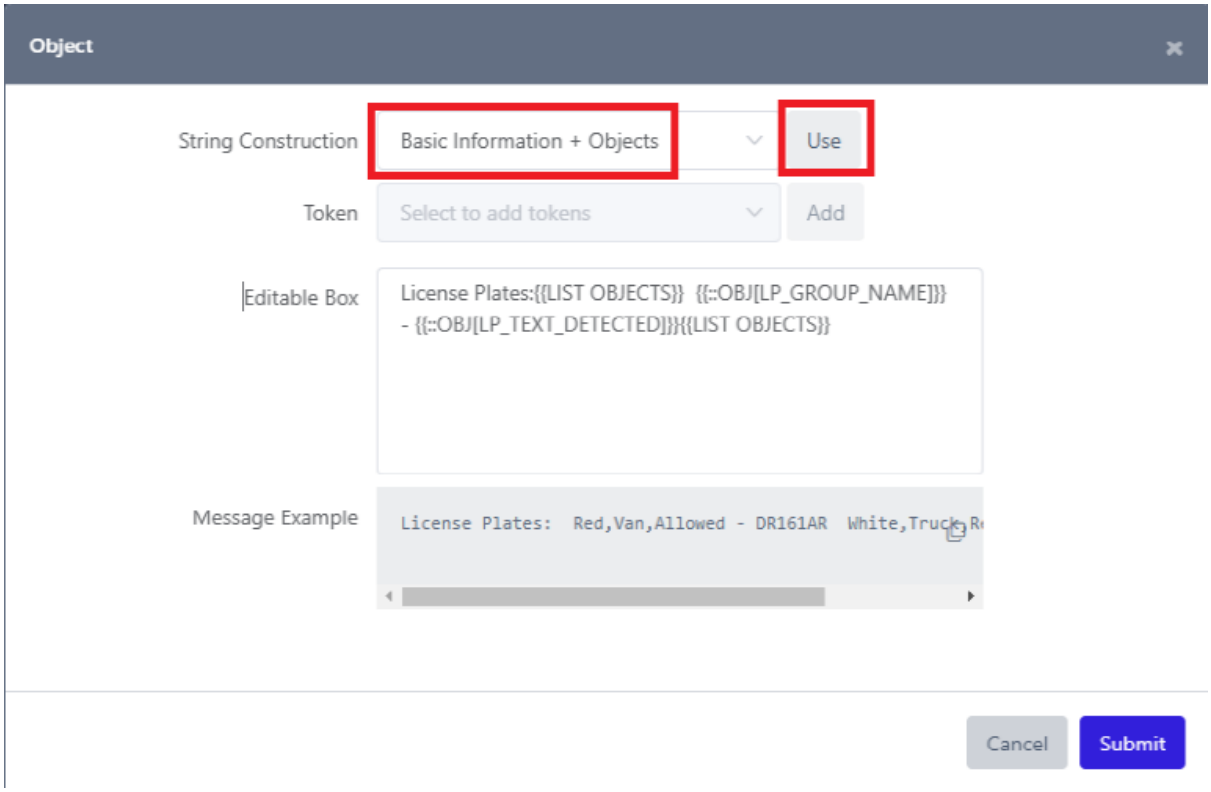
2.4 Set Event Action Message

With the Event Action message, you can configure the message format that is sent to Cortrol when an event occurs in AIBOX. For example, you can add LPR information or counting data to the message, which can then be viewed in Cortrol.

Click the“Set” button to configure the Event Action Message.

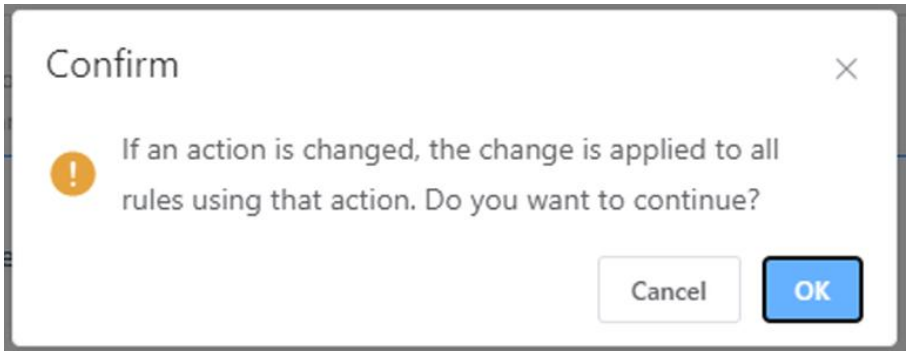


Select the desired event message, then click 'Use' to configure the event action message.



Note. In Control version 1.27.0.1366, there are multilingual issues and line breaks are not recognized properly, so data must be sent in a single line.

Click the **"Apply"** button to save the Control Server settings.

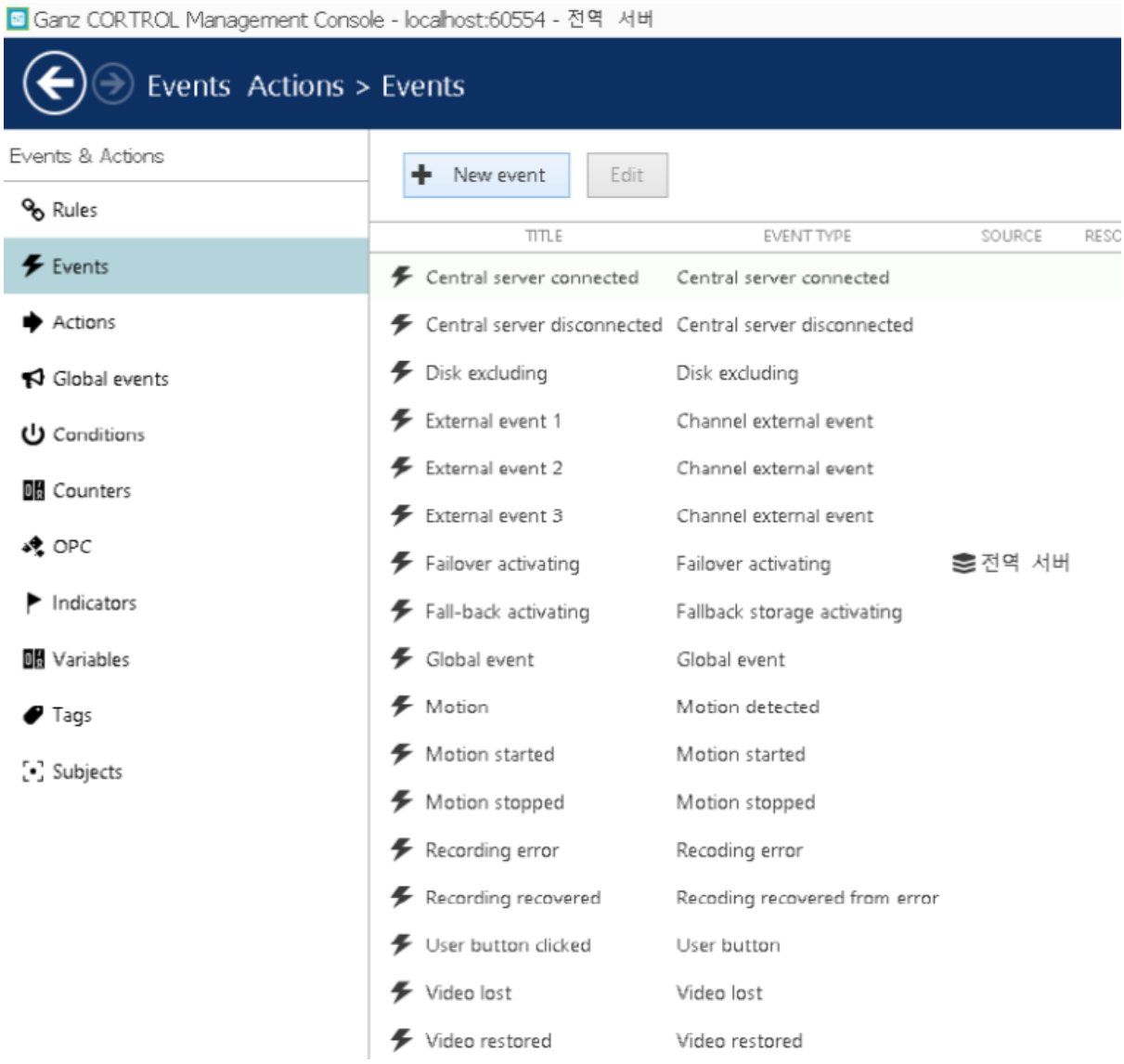


If you see the device registered in the format **"AIBOX-MacAddress"** in the External Service tab of the Cortrol Management Console, it's OK.

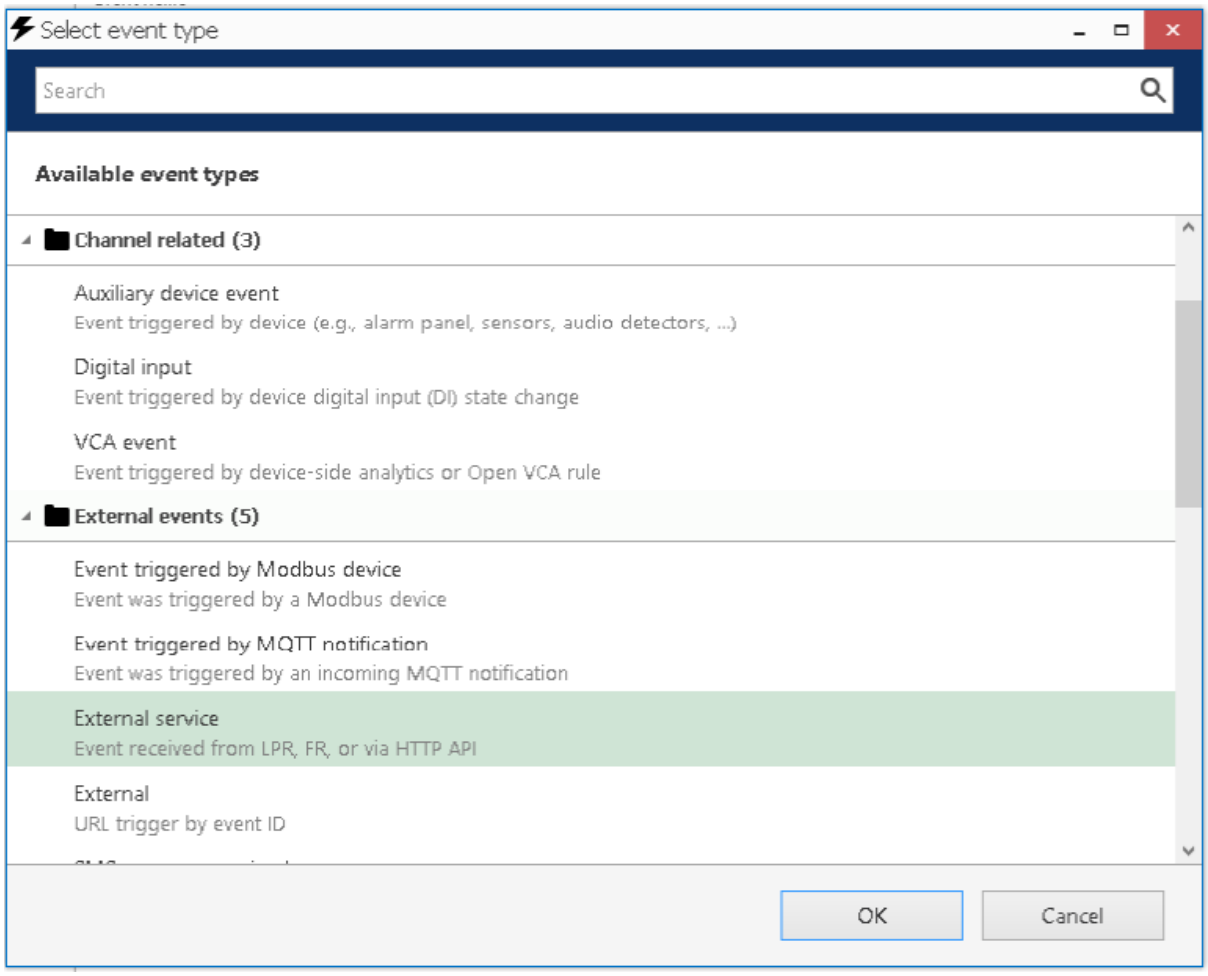
2.5 Create Cortrol Event & Rule

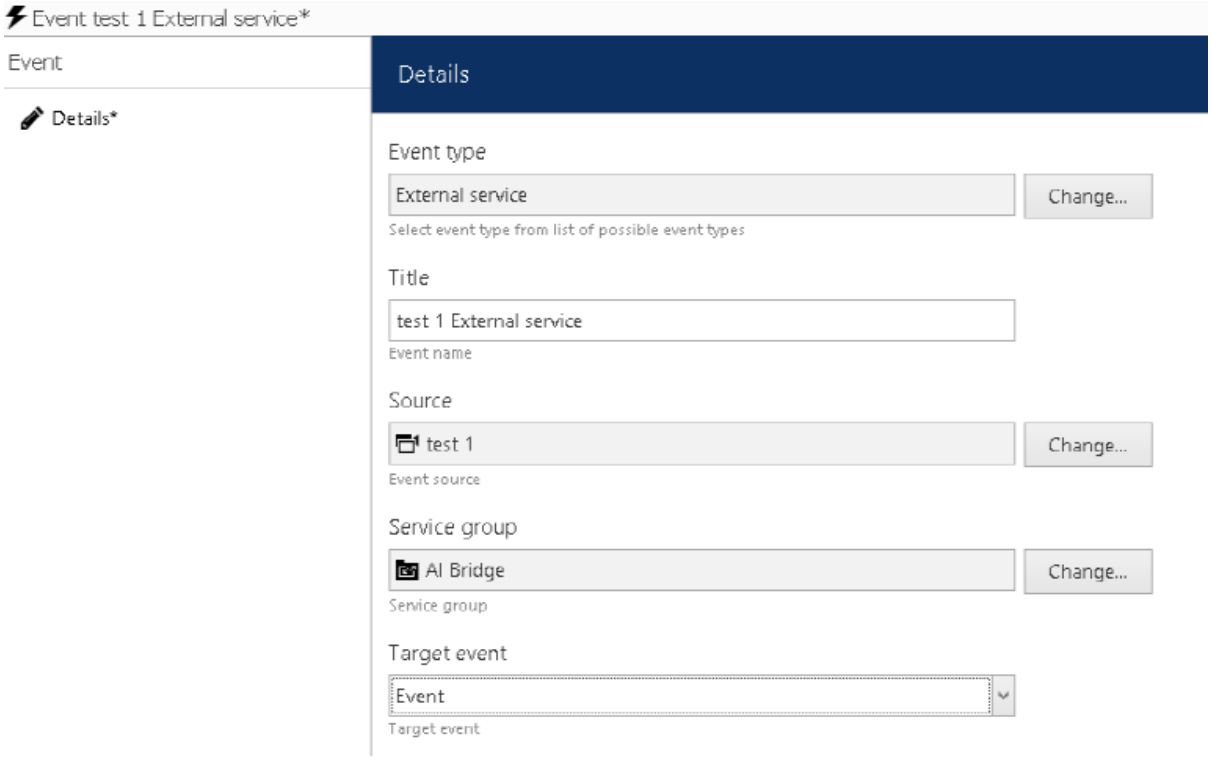
We need to configure the events, actions, and rules that will be sending notifications

Click the **"New Event"** button to add a new event.

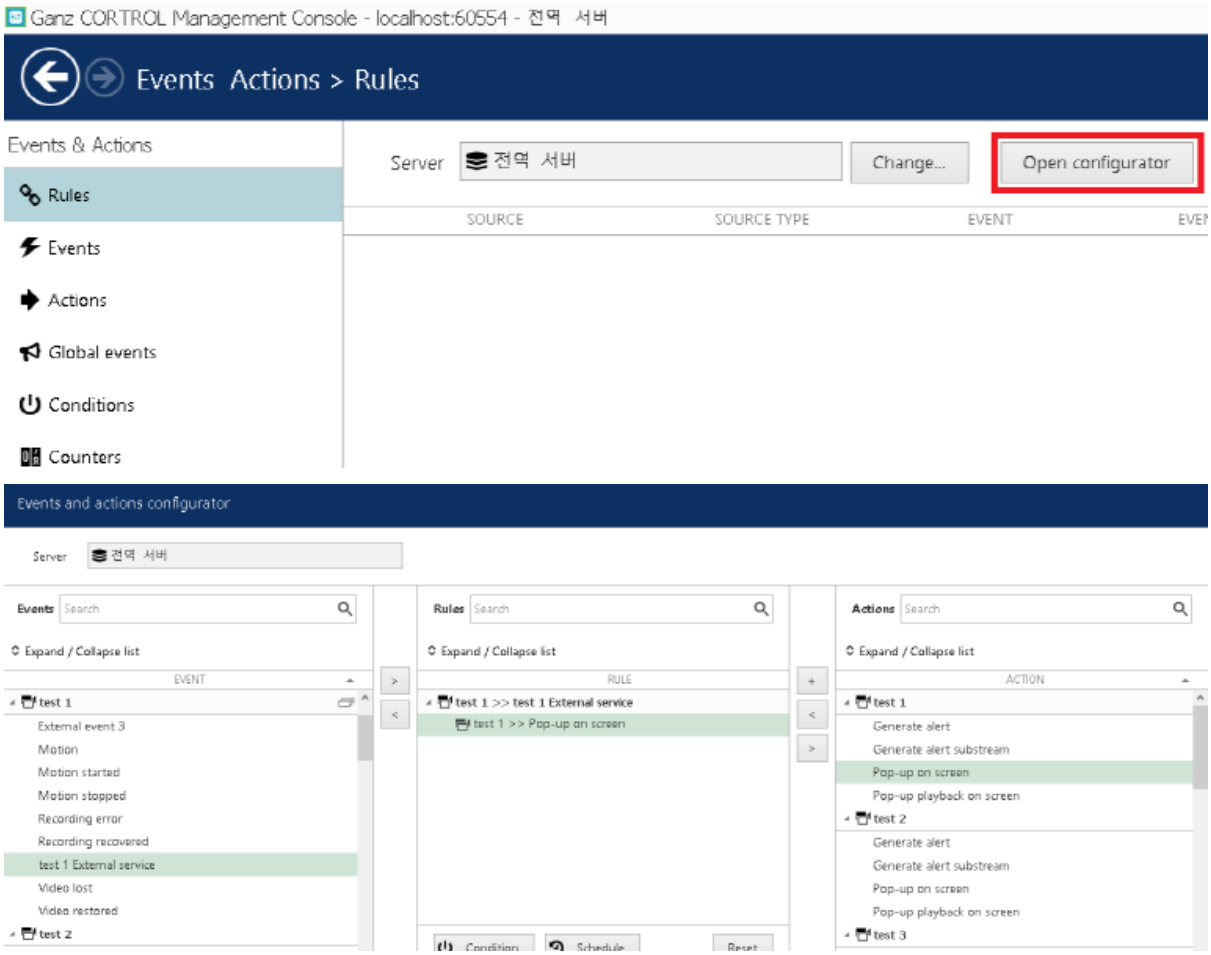


Select Event Type as **External Event – External Service.**





Create a rule by combining the created event type and action.



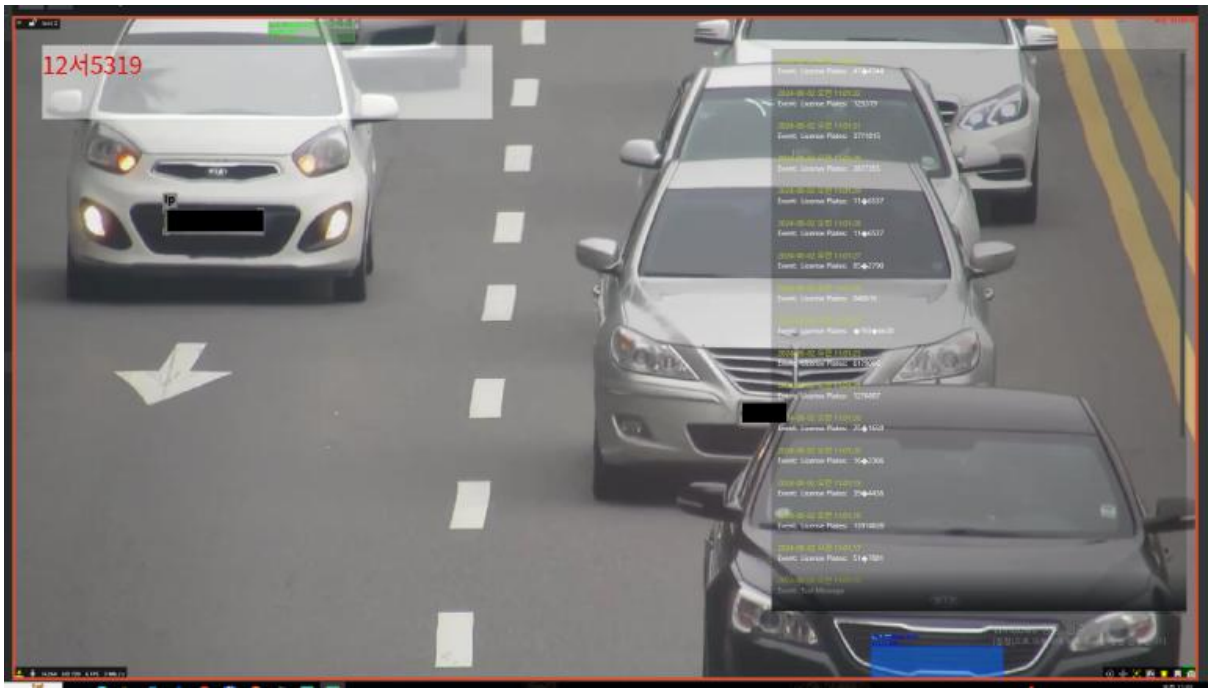
3. Demo

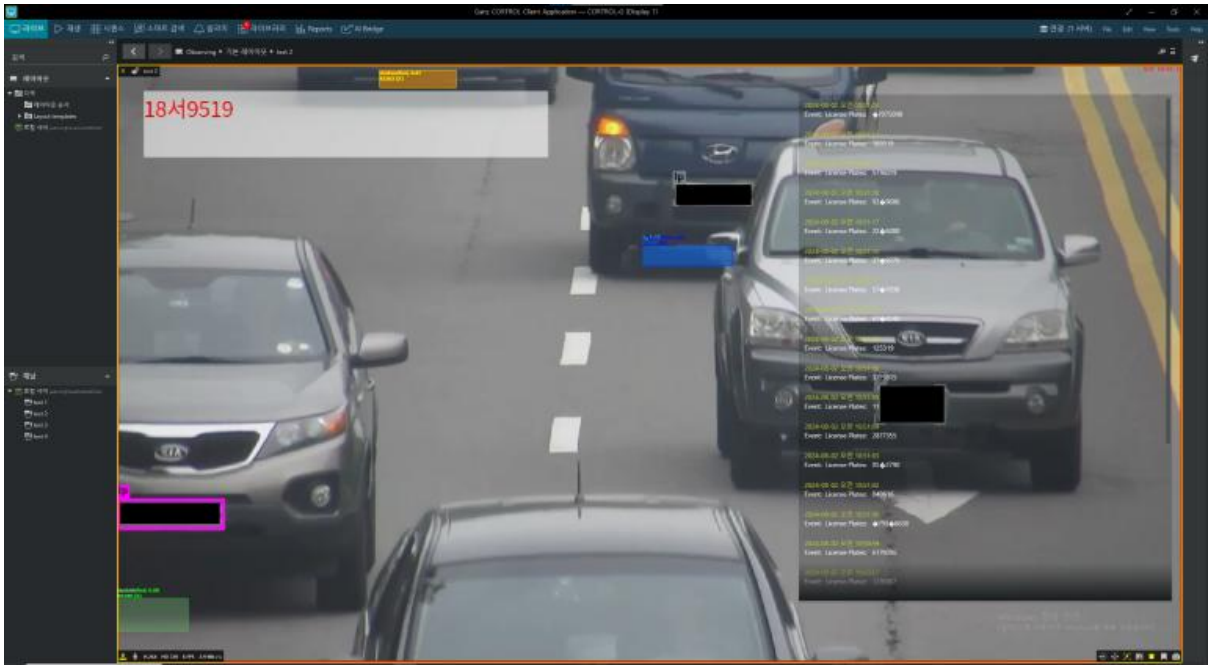
3.1 Live

Set the Cortrol Client to display metadata and alarms to check if it works with AIBOX.

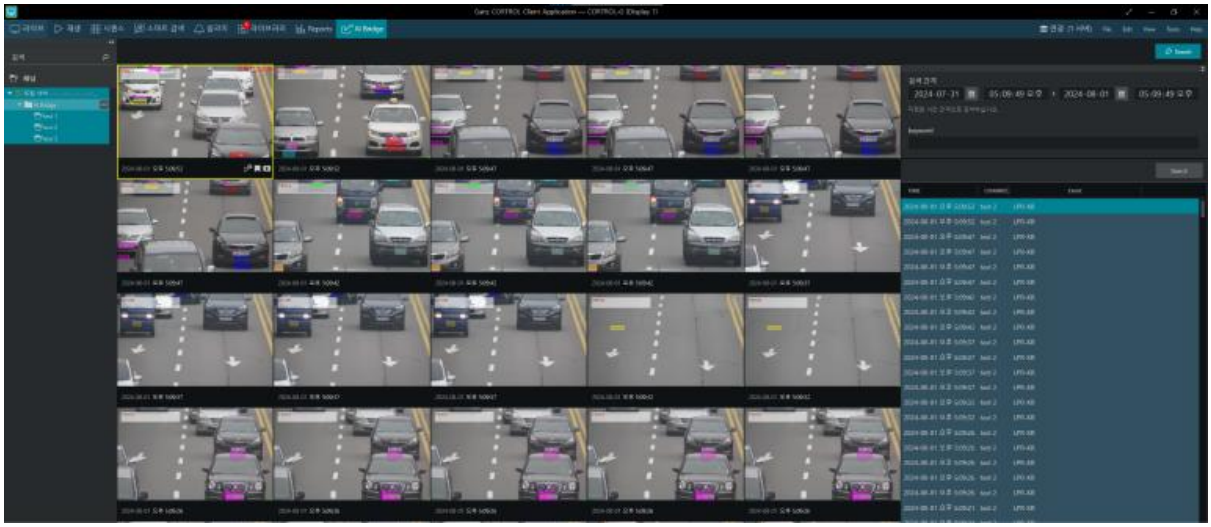
Click the icon at the bottom of the video.


12서5319


12서5319



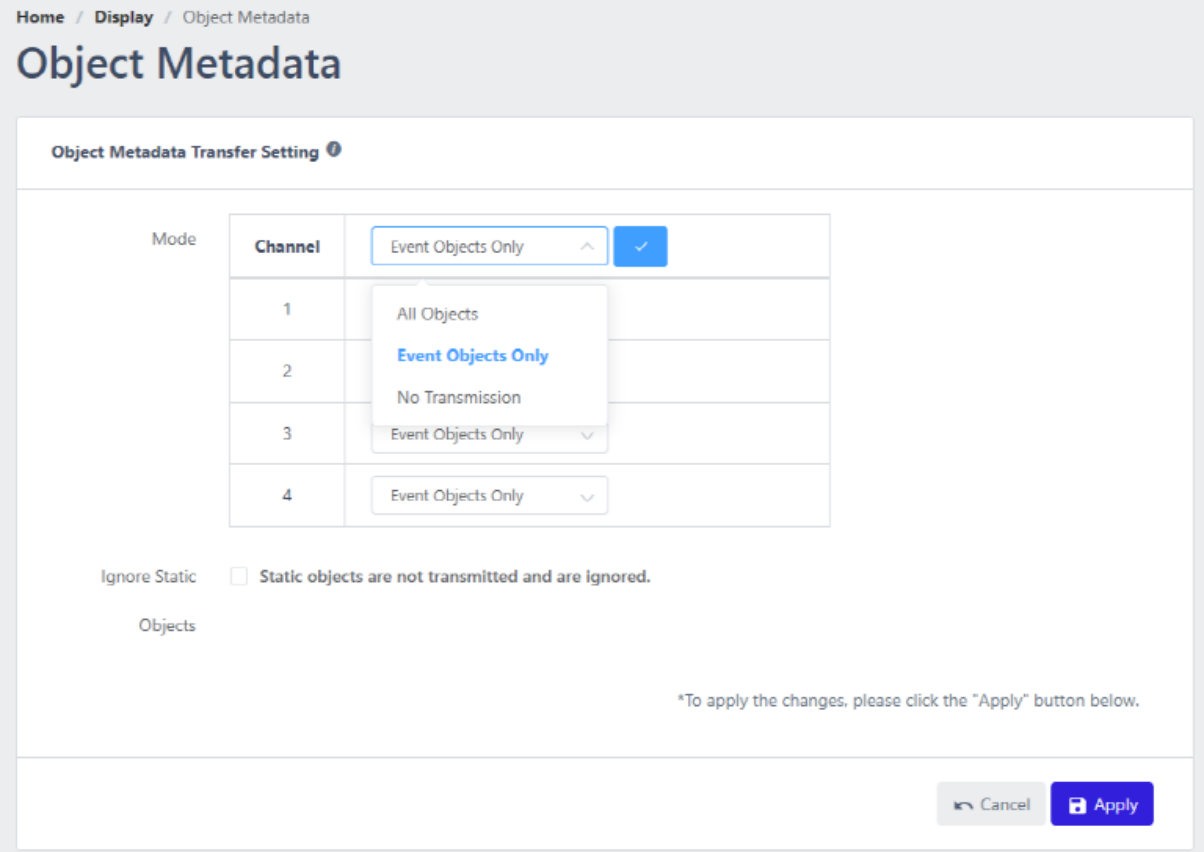
3.2 Search



4. FAQ

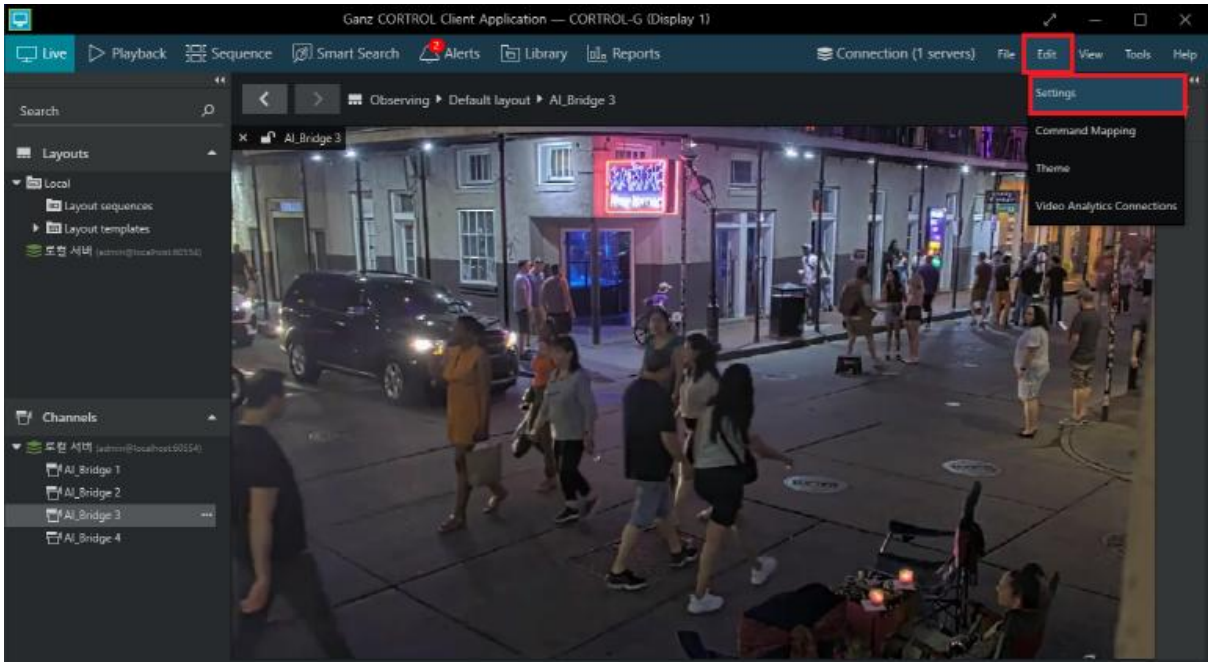
4.1 Object Metadata Transfer Options

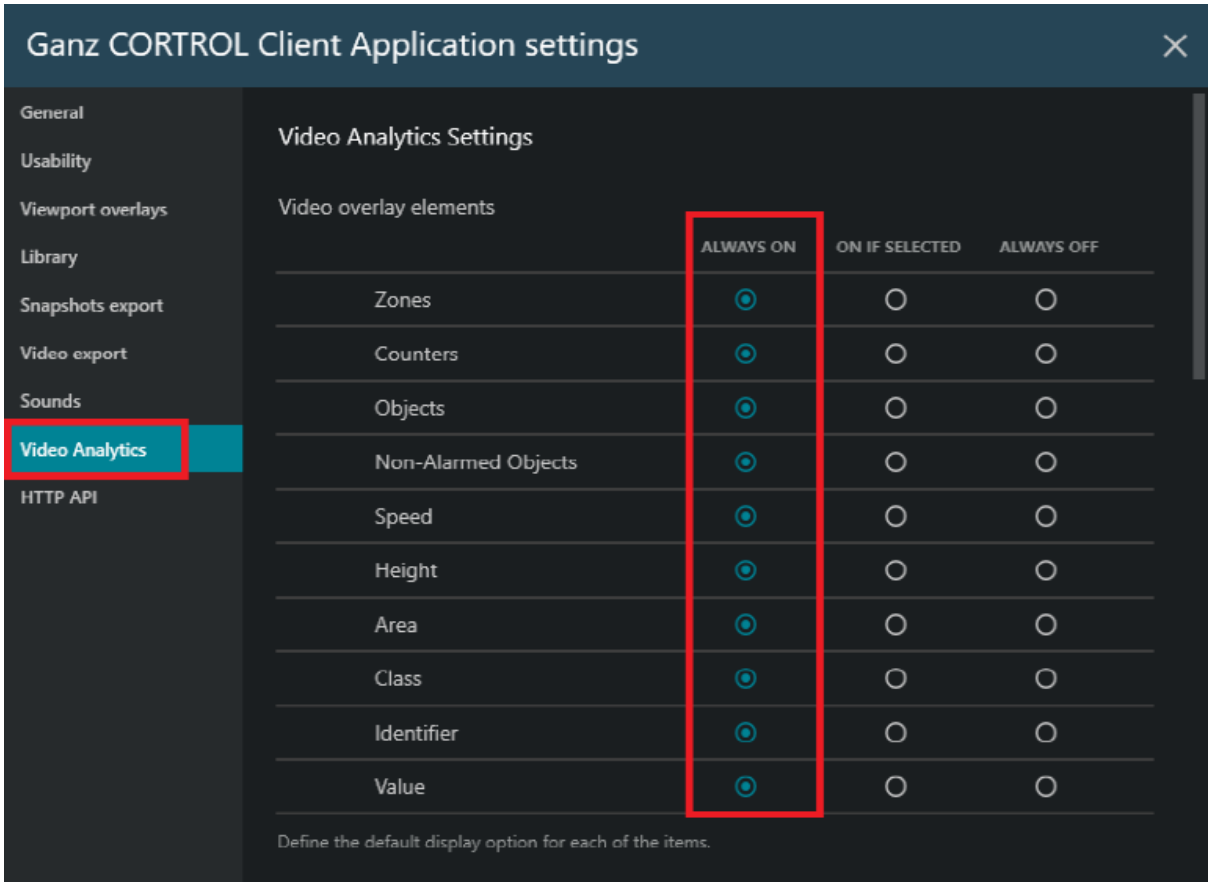
If this feature is turned OFF, ONVIF Metadata and the Metadata set in the Plugin will not be transmitted. This applies to the overall operation of Metadata.



4.2 Cortrol Client Side Video Analytics Overlay Settings

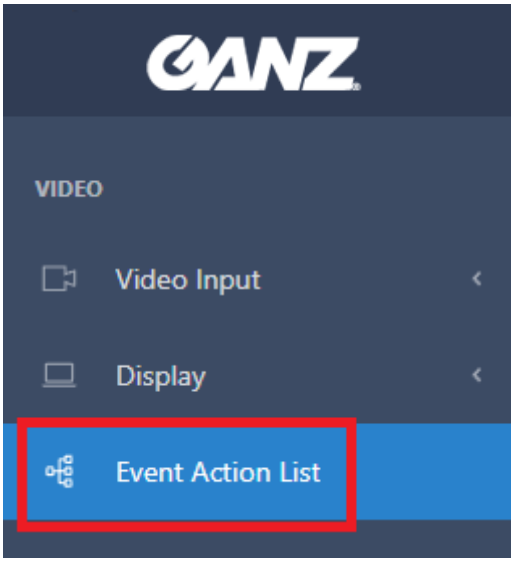
If Video Analytics is not enabled in the Settings under Edit in the Cortrol Client Application, metadata may not function correctly. The default value is ON, so do not turn this feature off.



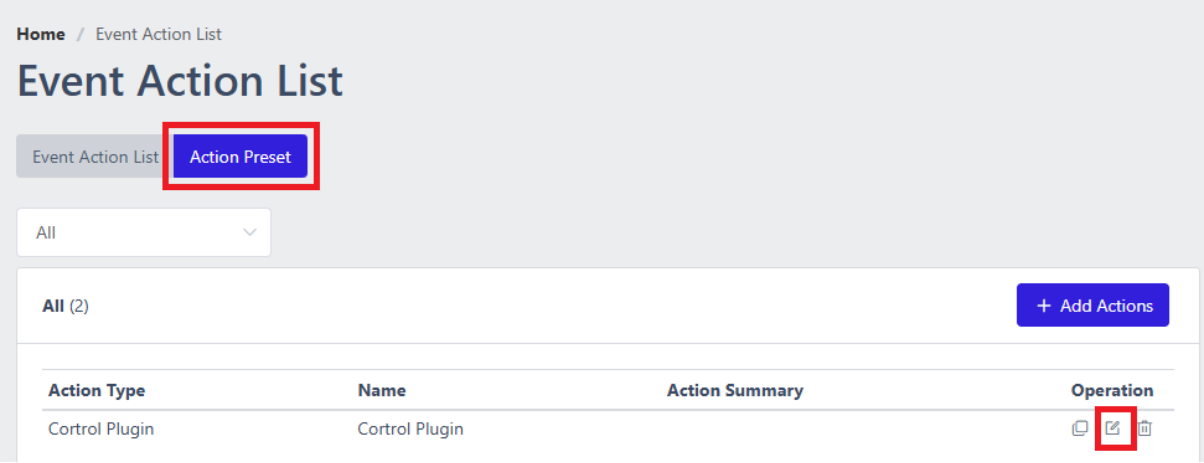


4.3 Check the connection between AIBOX and Cortrol

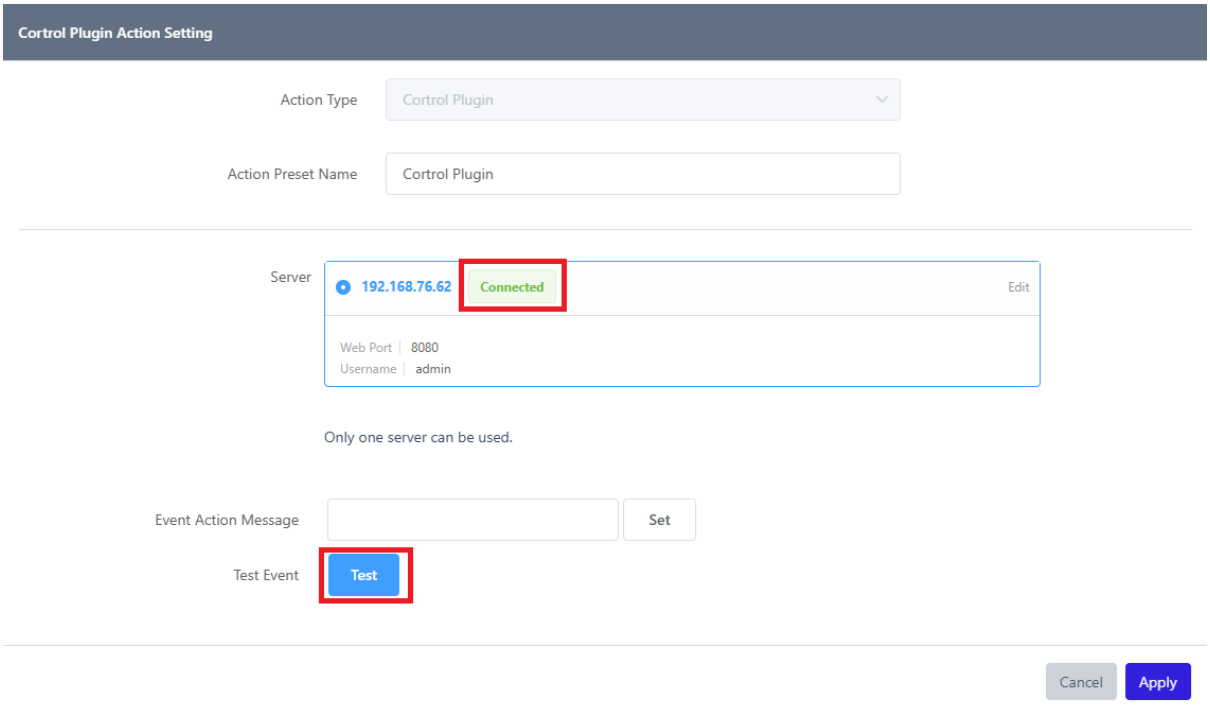
Click on “Event Action List” under “VIDEO” in the AIBOX webpage.



Enter “Action Preset” and click the Cortrol Plugin settings button that was configured earlier.

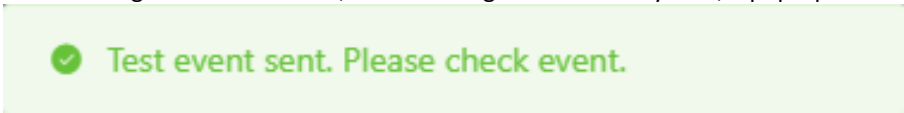


If it is confirmed that you are connected to the Control Server, click the “Test” button.

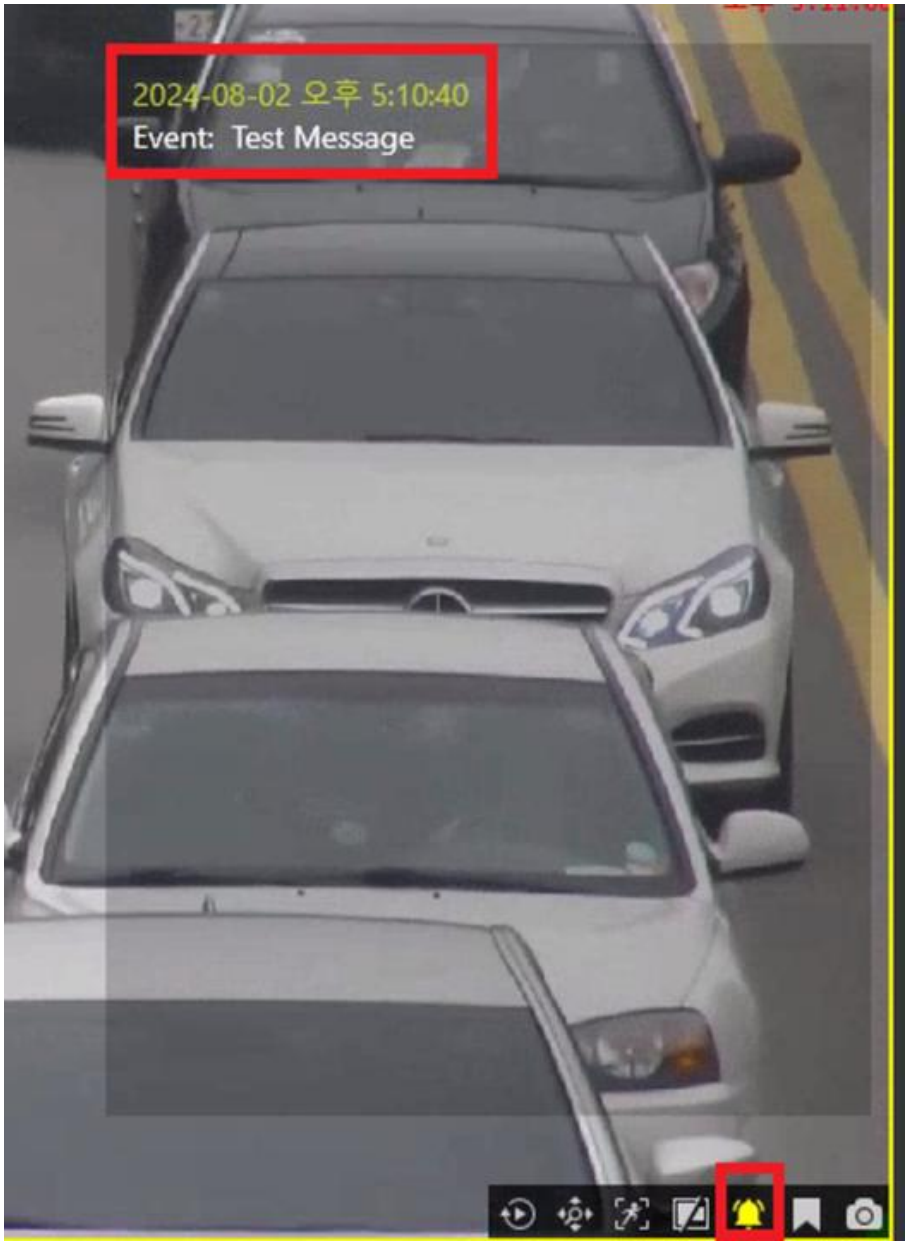


Note. Before clicking the TEST button, ensure that the green Connected button is visible on the Control Server. If the gray Disconnected indicator is displayed, please check the server settings.

After clicking the “Test” button, if the message is successfully sent, a pop-up like the one below will appear.



Now, go to Control and check the alarm message.



Genetec Integration Guide

1. Introduction

1.1 Prerequisites

- AIBOX FW version 1035xx or higher.
- Genetec Security Center 5.11 higher.

1.2 Learn about integration architecture

There are two ways to integrate AIBOX with Genetec VMS:

1) Case 1

AIBOX receives the RTSP video stream from the IPCAM and processes it to provide annotated videos and event data after AI analysis. The video is transcoded to include object recognition data, bounding boxes, zone information, and more.

2) Case 2

Both AIBOX and Genetec VMS simultaneously receive the RTSP stream from the IPCAM. AIBOX sends the AI analysis events directly to Genetec VMS and can also source the RTSP stream from Genetec VMS instead of directly from the IPCAM.

Among Case1 and Case2, this guide will explain how to integrate using Case1.

2. Configuration

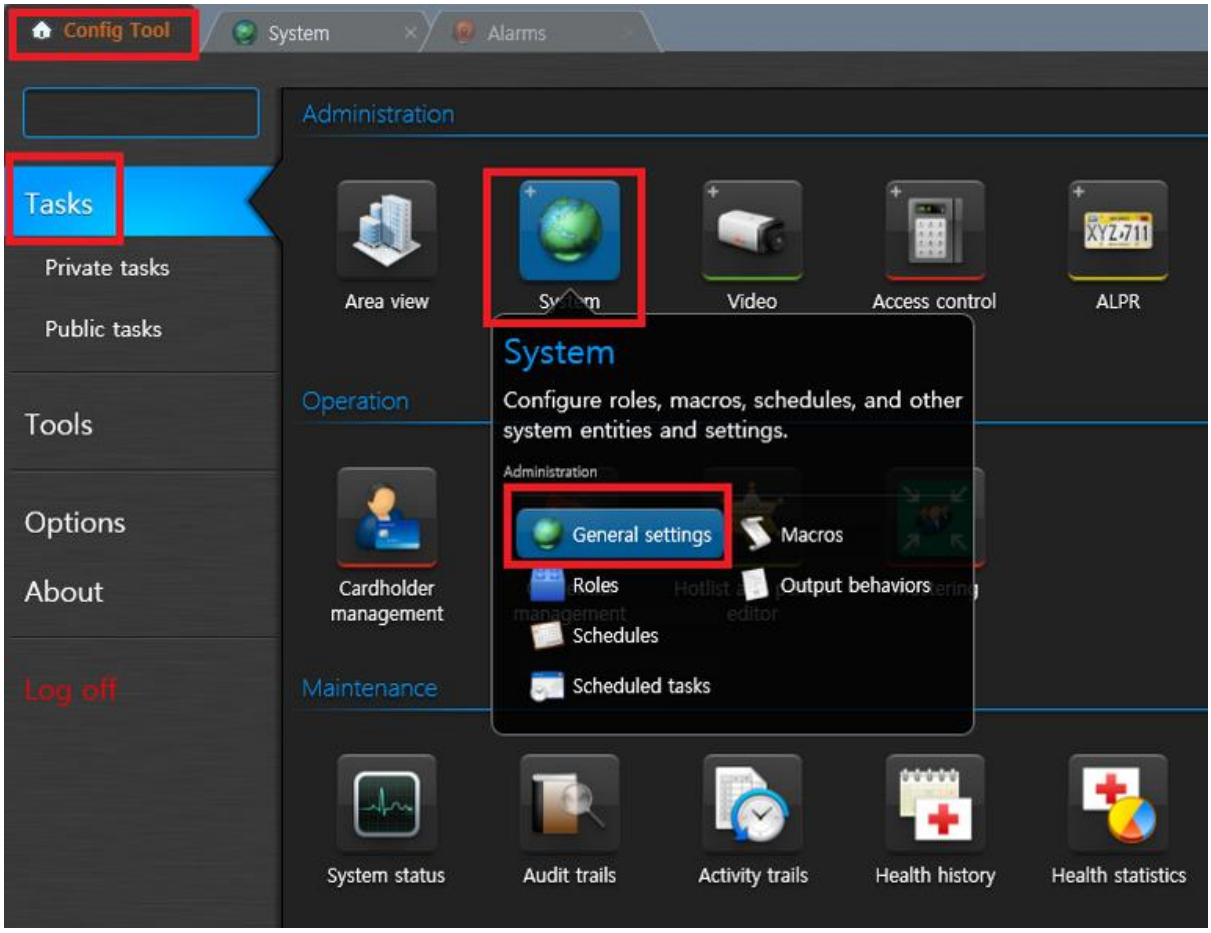
To integrate events between AIBOX and Genetec, WebSDK registration, Genetec event configuration, and AIBOX configuration are required. The following explains each configuration method.

2.1 Setup the WebSDK

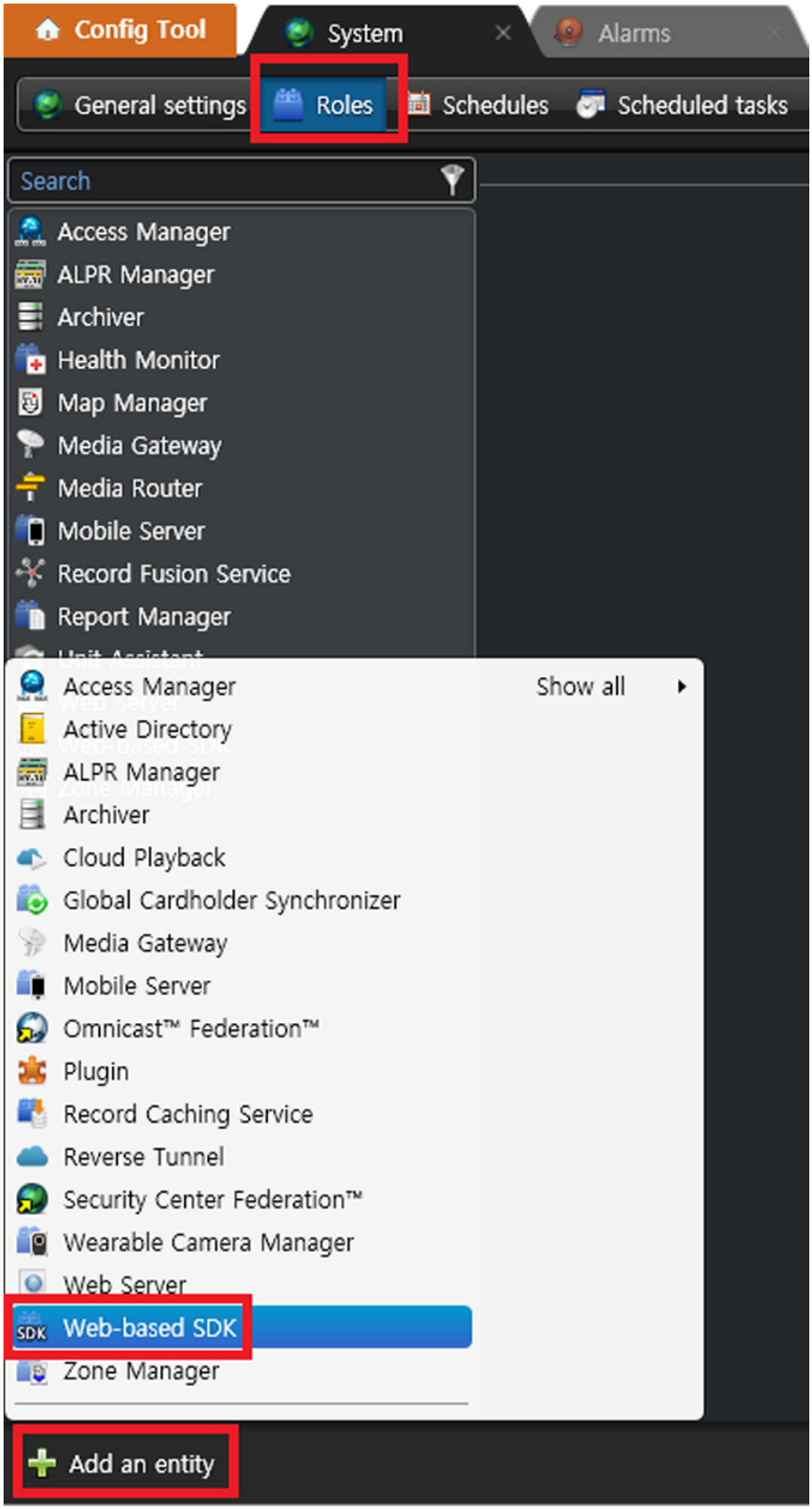
It is necessary to check whether it is a license that supports WebSDK function. If it is not, it does not work properly. In order to integrate AIBOX and Genetec, you need to purchase a WebSDK license.

Note. Must request a license from Genetec. (ex. GSC-1SDK-?????-??????)

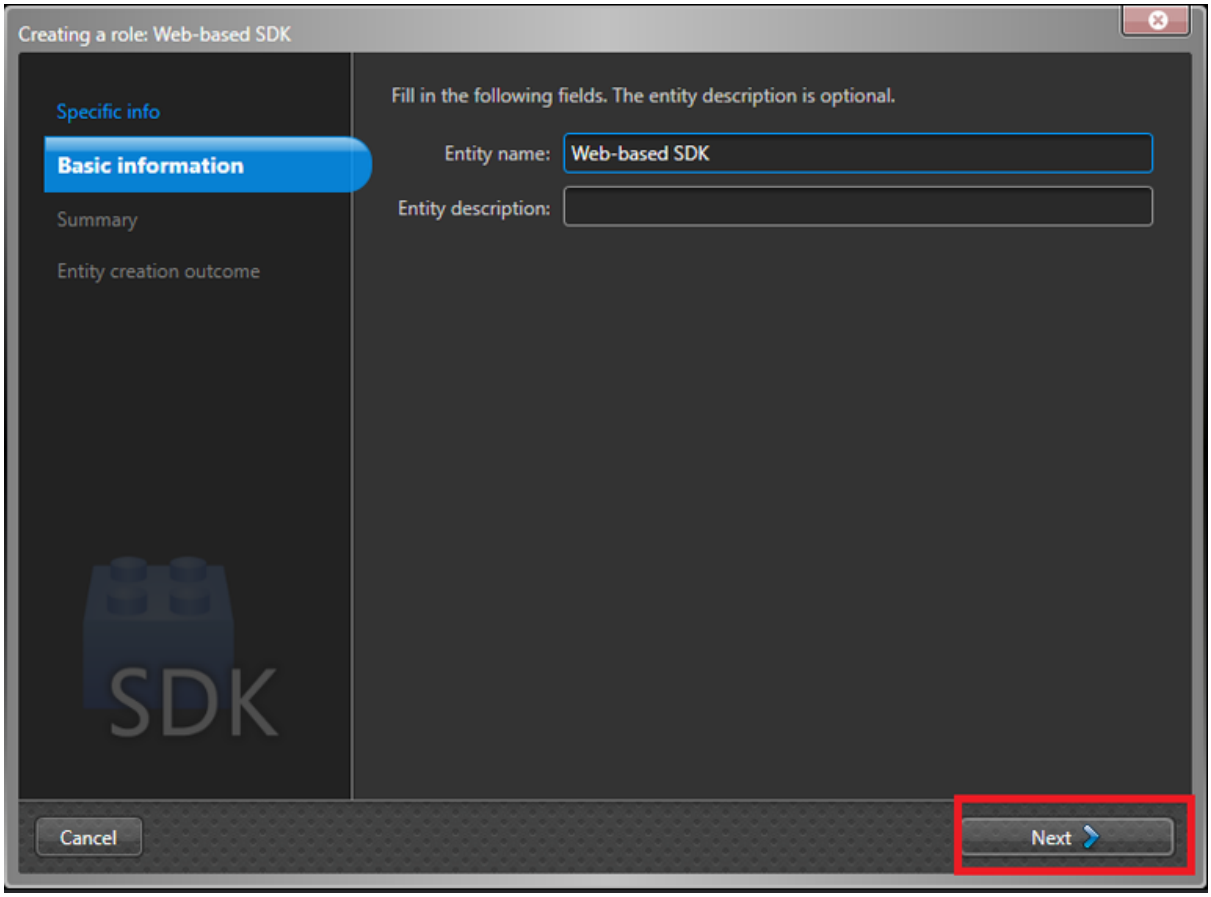
Config Tool > Task > System > General settings

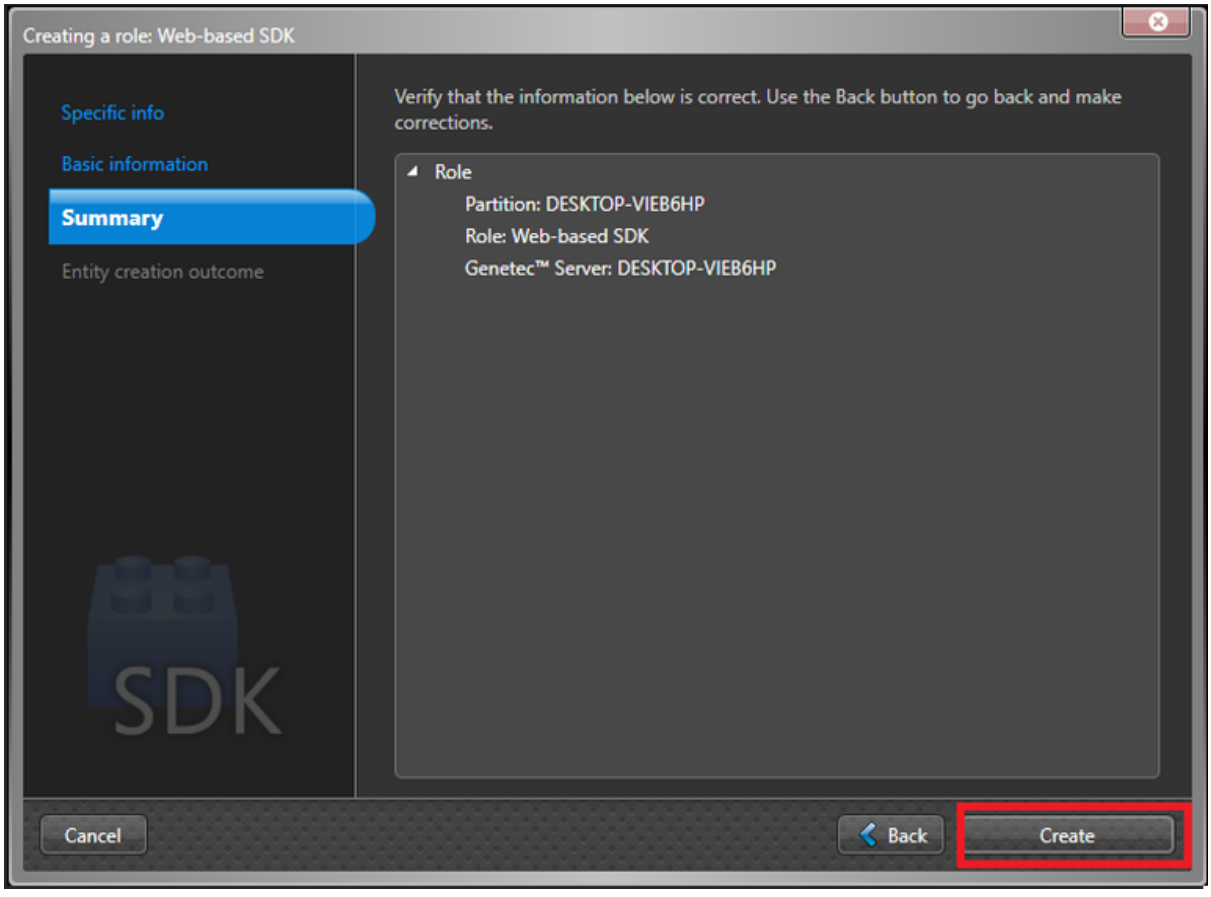


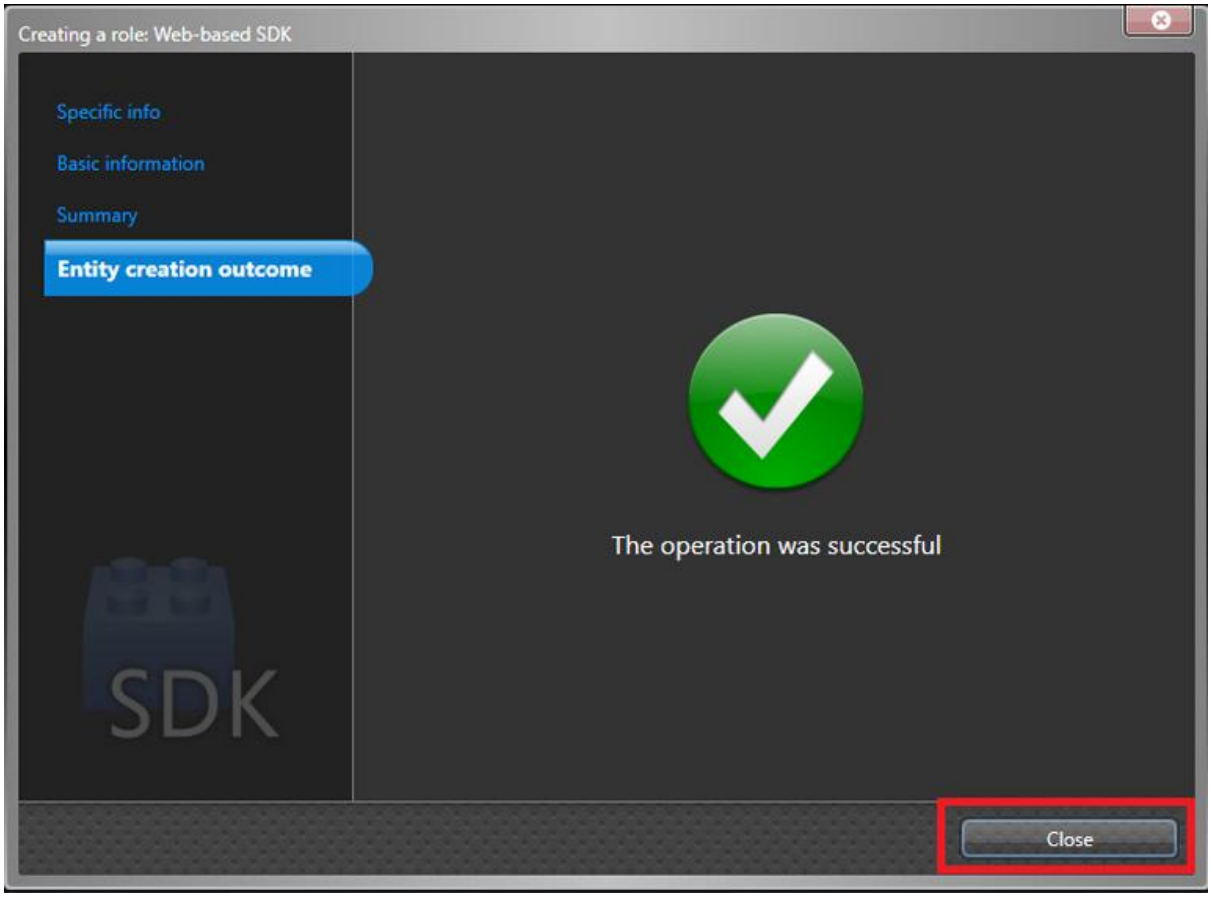
Access the Roles tab, click on ‘Add an entity’ at the bottom left, and add a Web-based SDK.



Process: Next > Create > Close

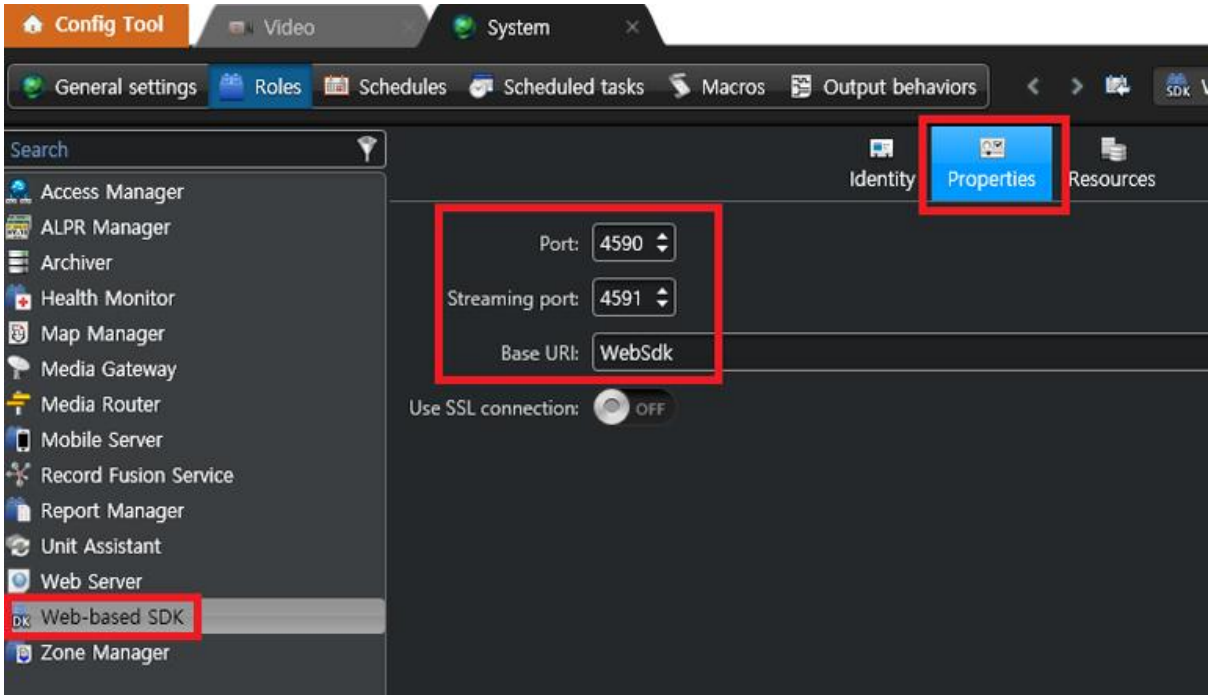

Creating a role: Web-based SDK
Specific info
Basic information
Summary
Entity creation outcome
Fill in the following fields. The entity description is optional.
Entity name:
Web-based SDK
Entity description:
SDK
Cancel
Next


Creating a role: Web-based SDK
Specific info
Basic information
Summary
Entity creation outcome
Verify that the information below is correct. Use the Back button to go back and make corrections.
Role
Partition: DESKTOP-VIEB6HP
Role: Web-based SDK
Genetec™ Server: DESKTOP-VIEB6HP
SDK
Cancel
Back
Create



Enter the desired port number.

Tip : If the event is not working properly, check the firewall.



2.2 Genetec Configuration

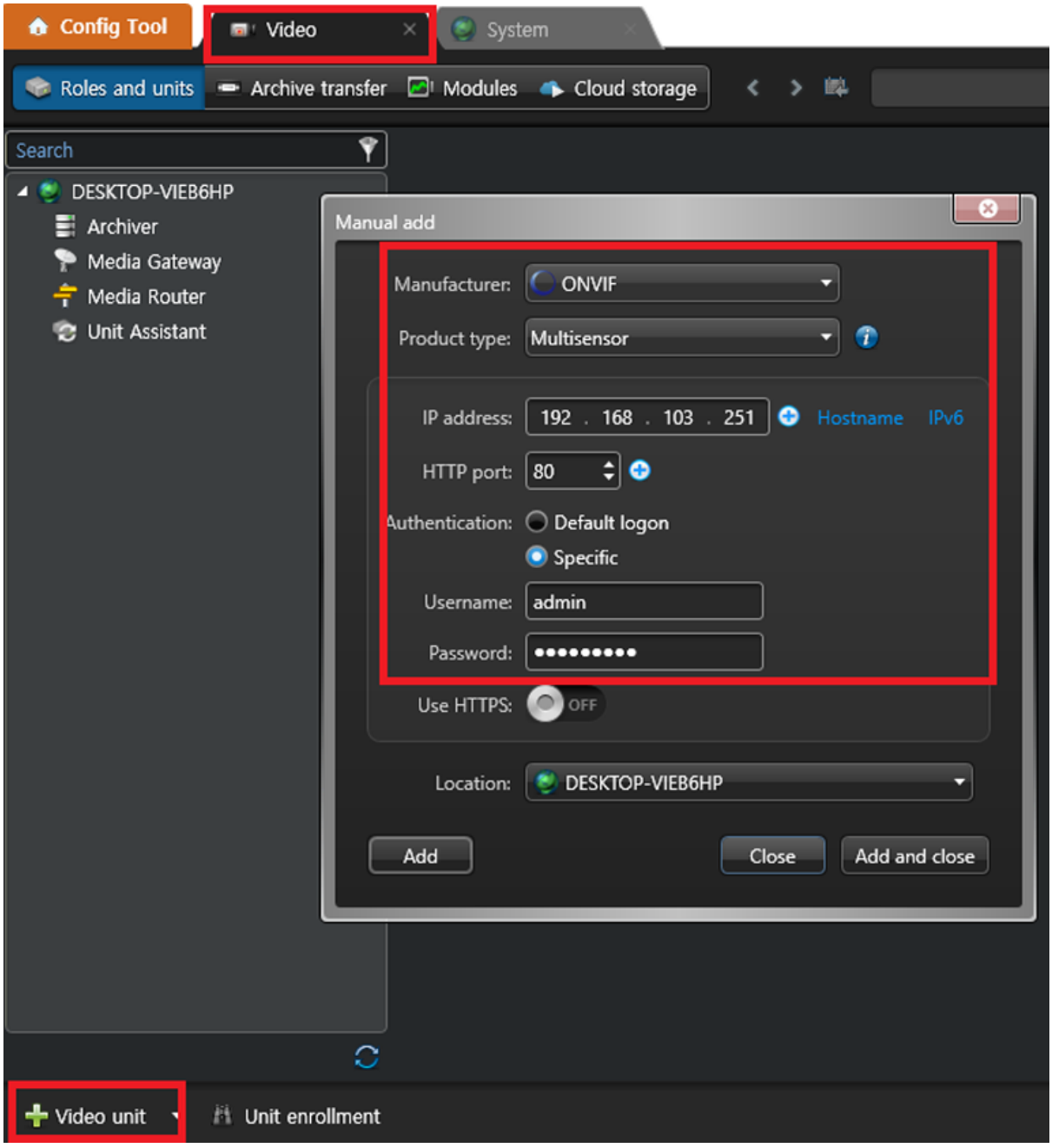
2.2.1 Adding Device

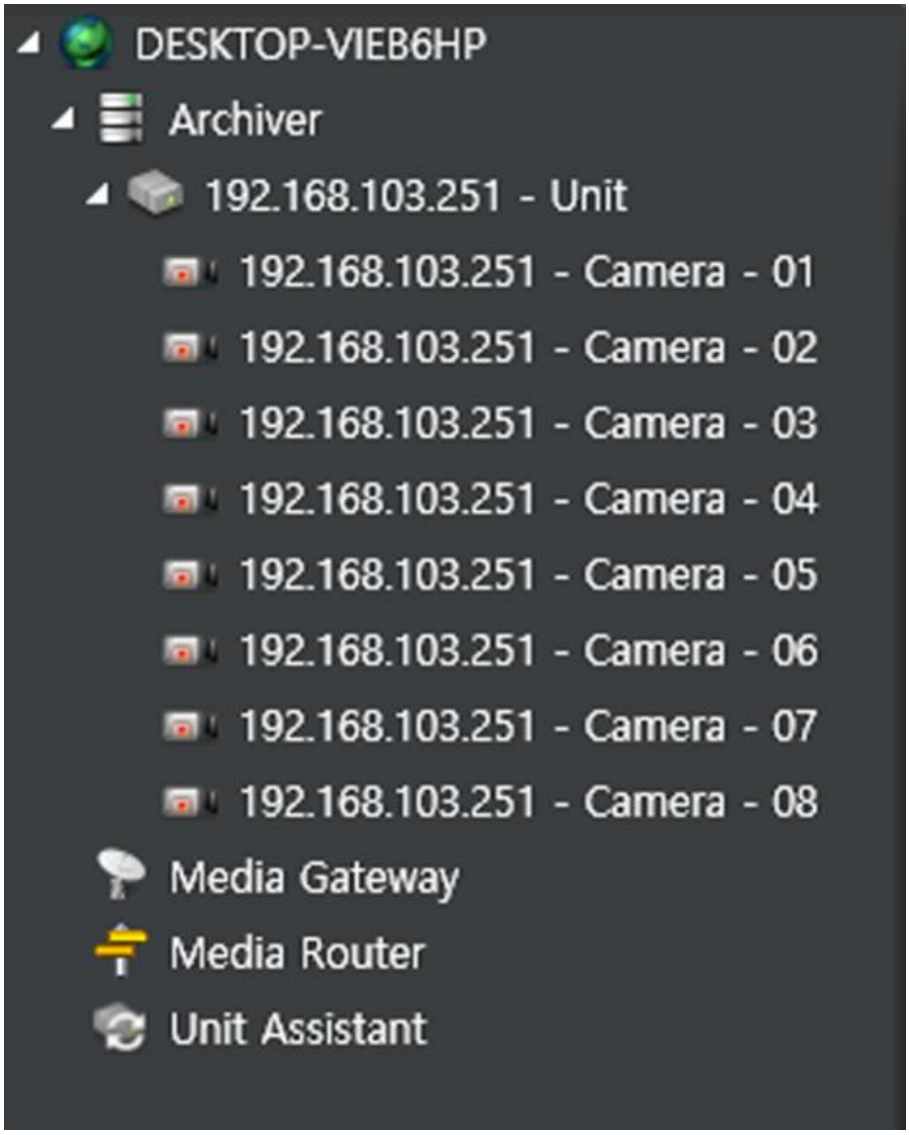
To use the annotated video, you must first add the device. The following explains how to add the device.

If you are not using the annotated video, you can skip this session.

Note : We have created this guide using Case1 because we prefer annotated video.

In the Video section of the Config Tool, add the AIBOX.

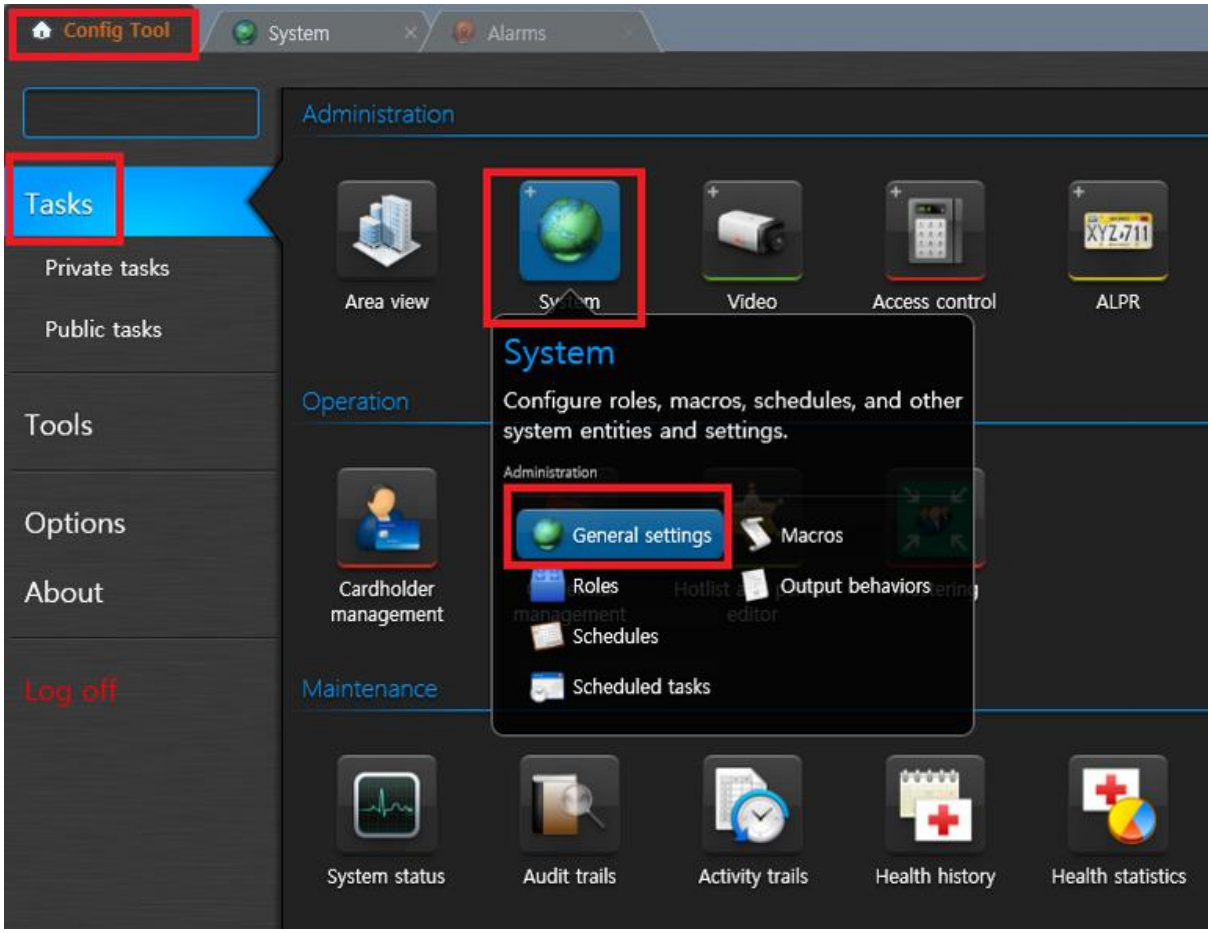




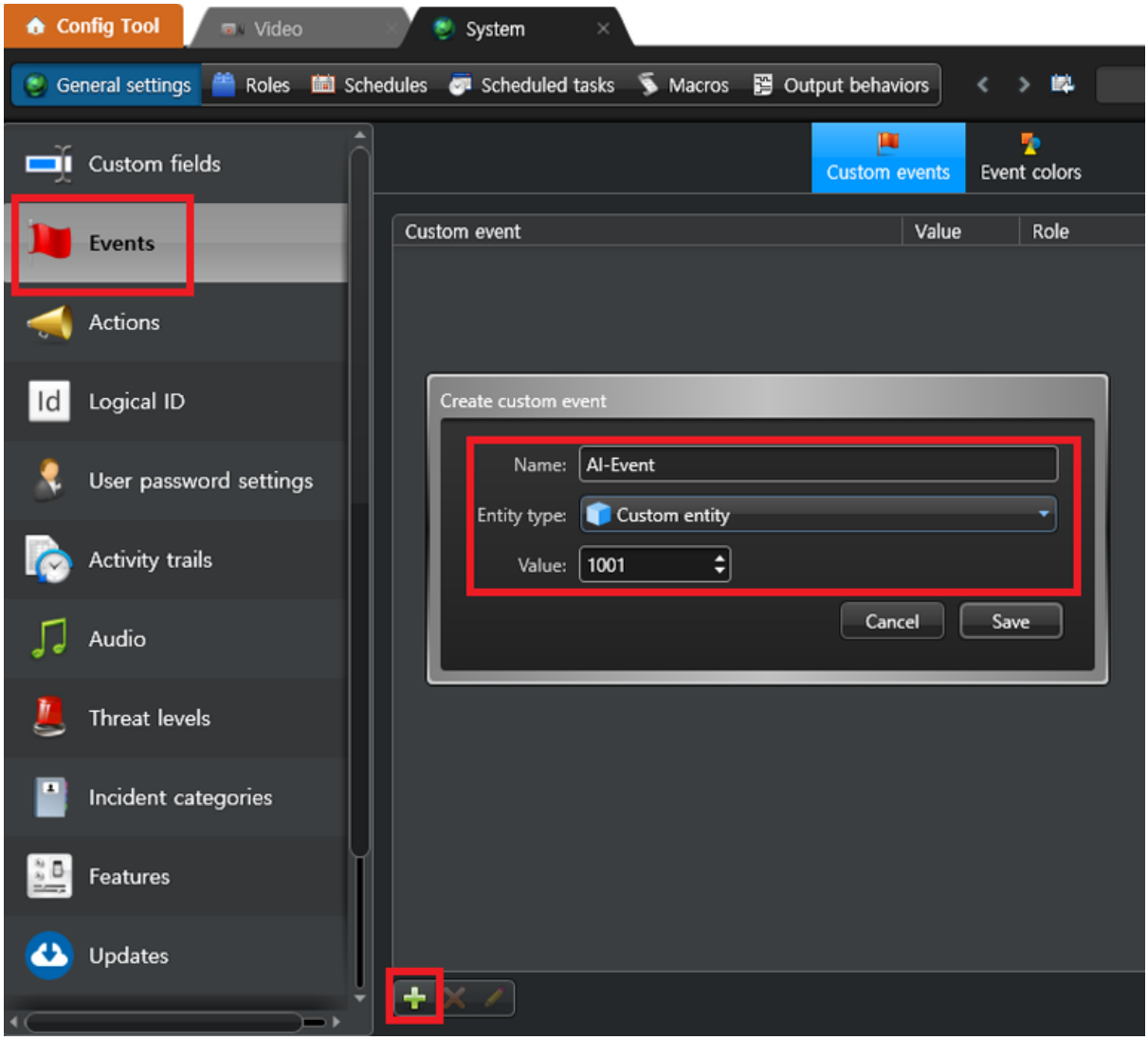
2.2.2 Event and Action Settings

Once the device registration is complete, follow these steps to register the AI Event in Genetec.

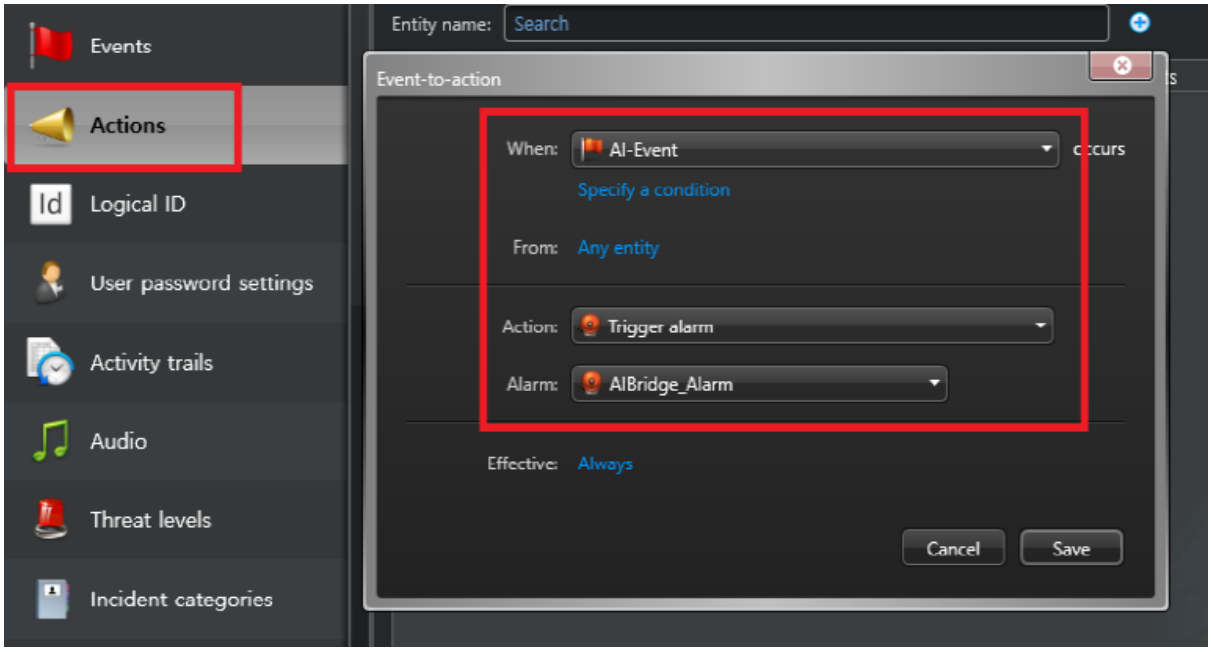
Navigate through: Config Tool > Task > System > General settings



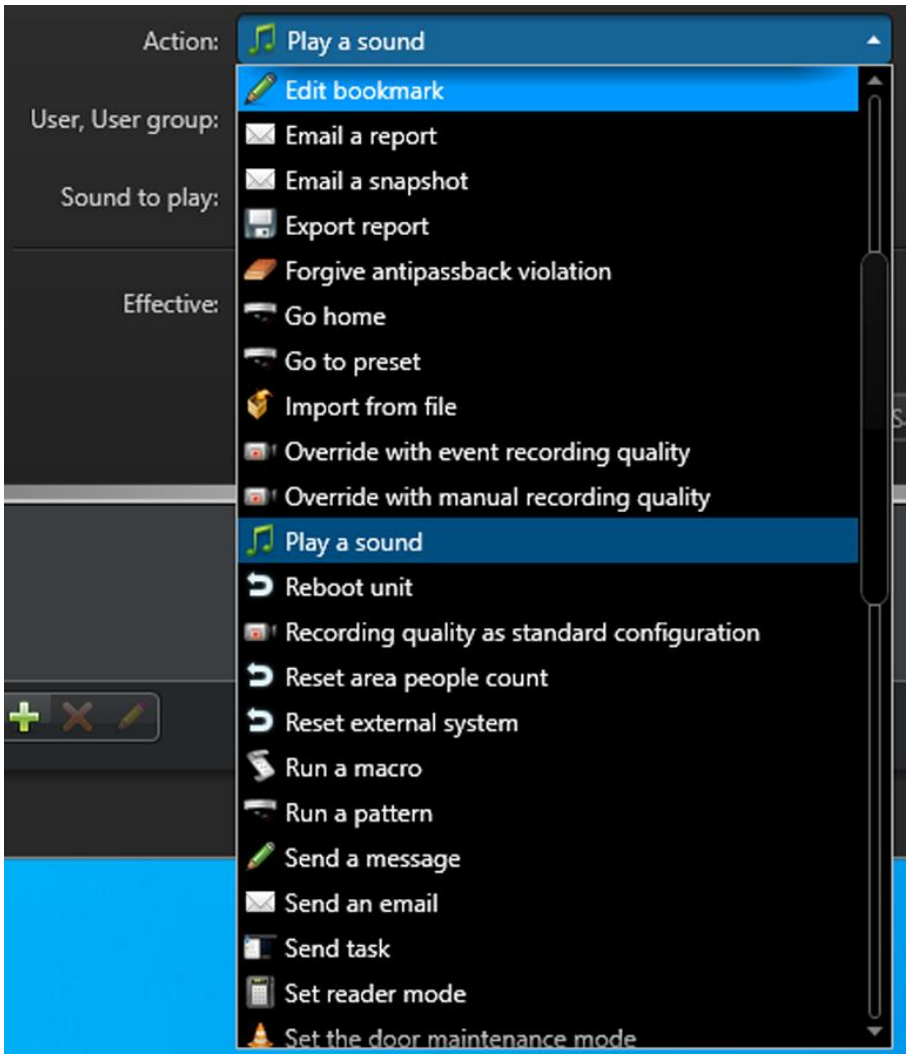
In the event panel, click the + button at the bottom left to add an AI-Event.



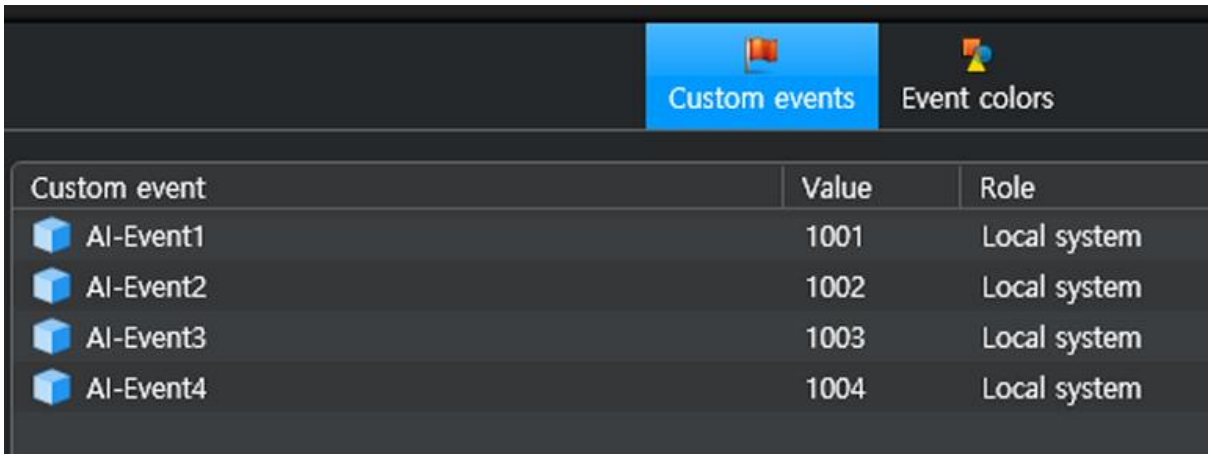
In the ‘When’ selection, select the AI Event created earlier. In the Action tab, select the desired Action and Camera. (ex. This guide uses bookmarks.)

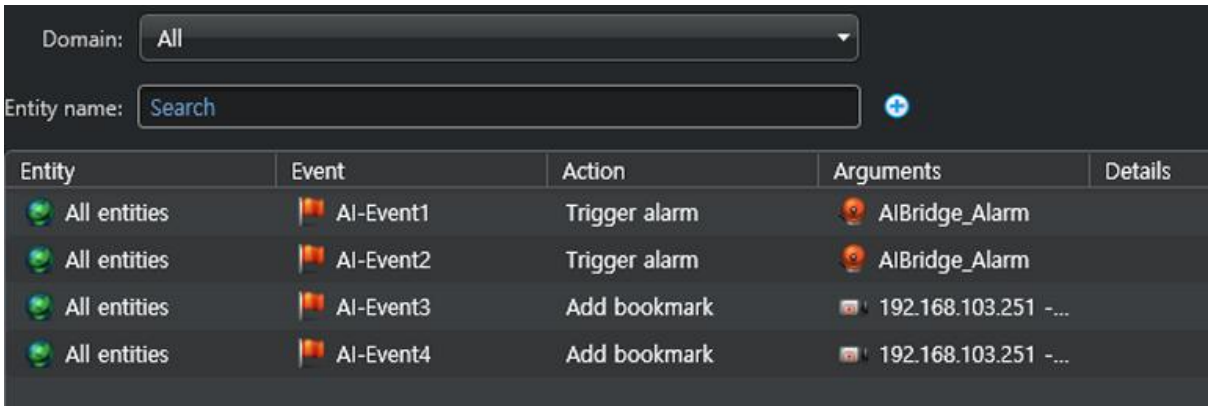


Note : As shown in the picture below, you can set various output events in the Action tab. Use them as needed.



If you want to use different Alarms for each AIBOX channel, you designate video channels for each channel and create alarms sequentially, as shown in the attached example.

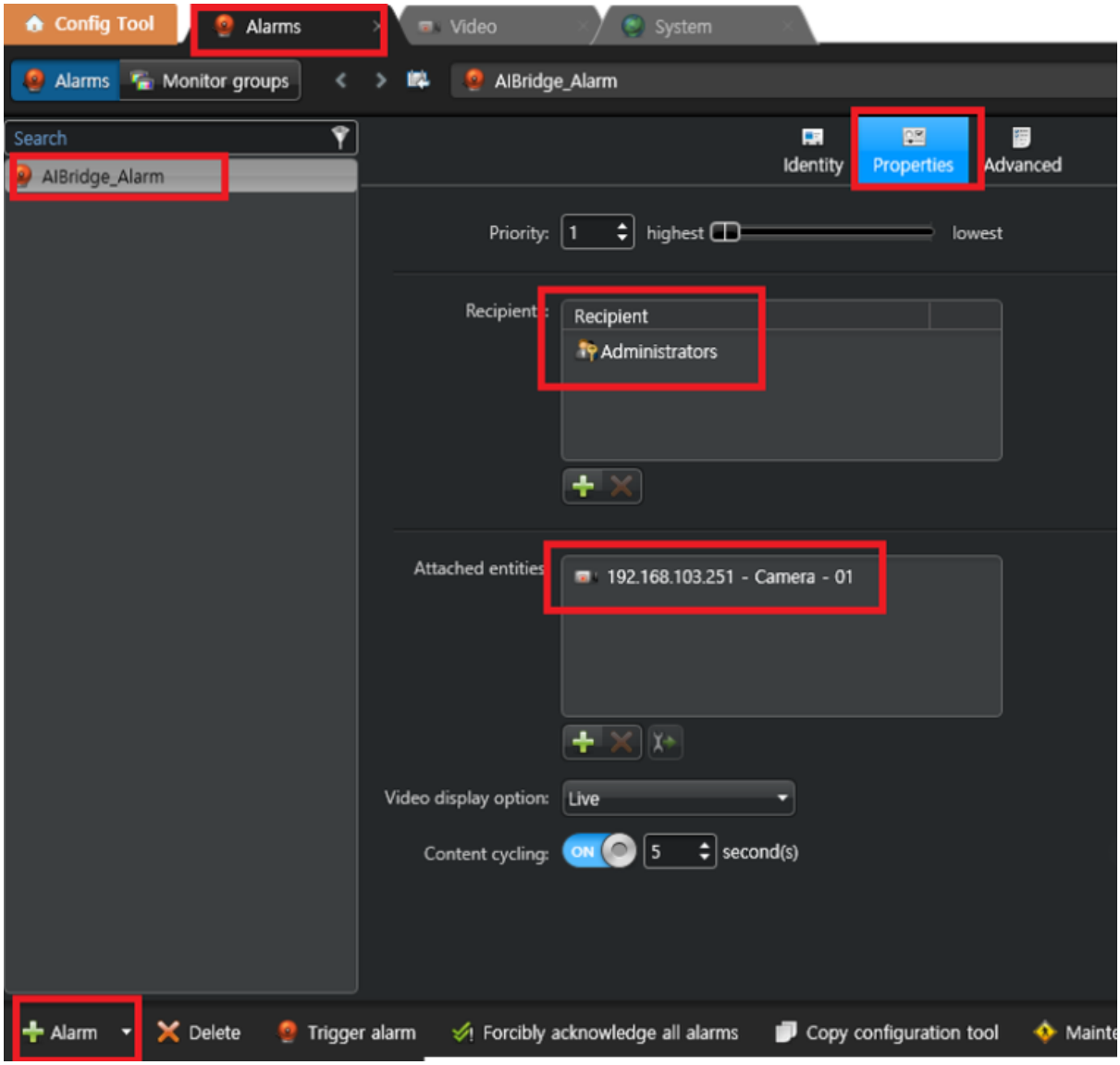




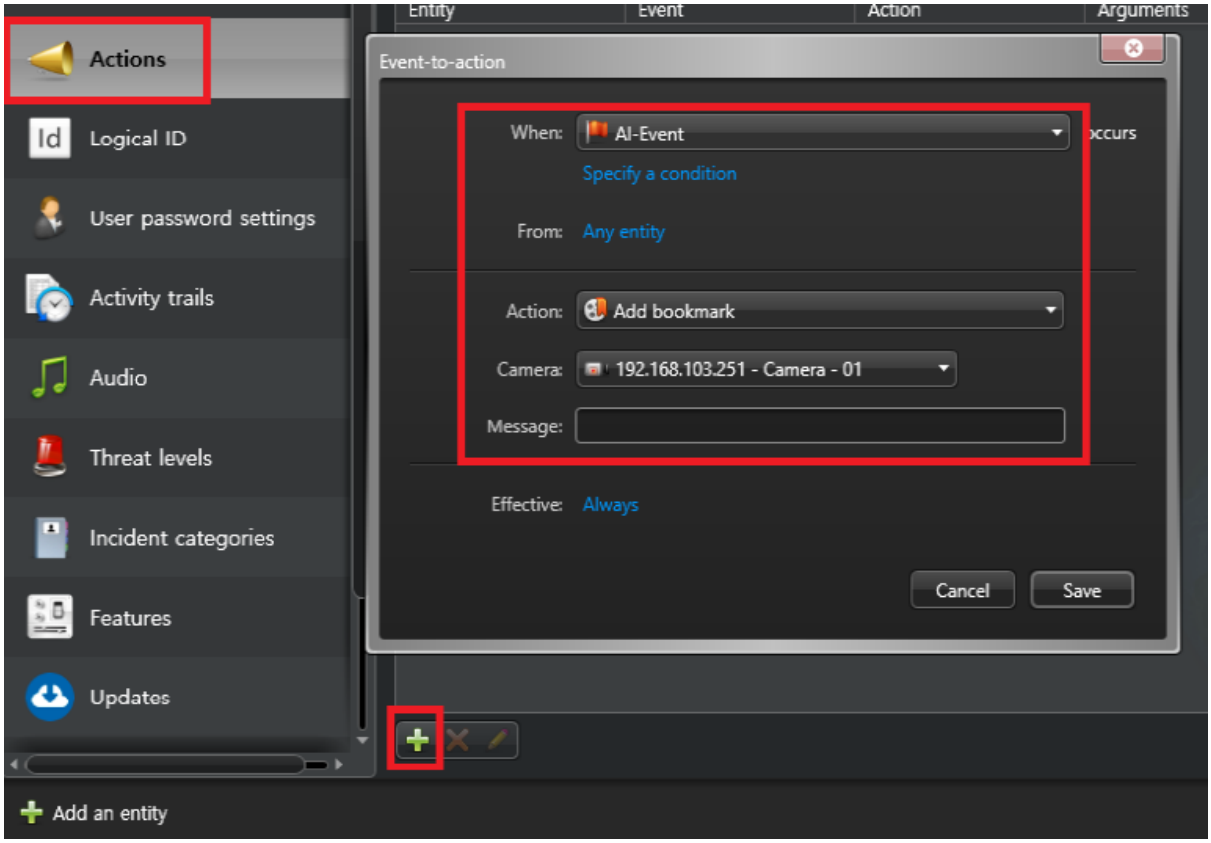
2.2.3 Alarm Monitoring Event Setting

Go to the Alarm tab in the Config Tool and set it up as follows.

Note : You can select cameras freely.



For the previously created AI Event, select Trigger Alarm, and for Alarm, select the alarm created above.

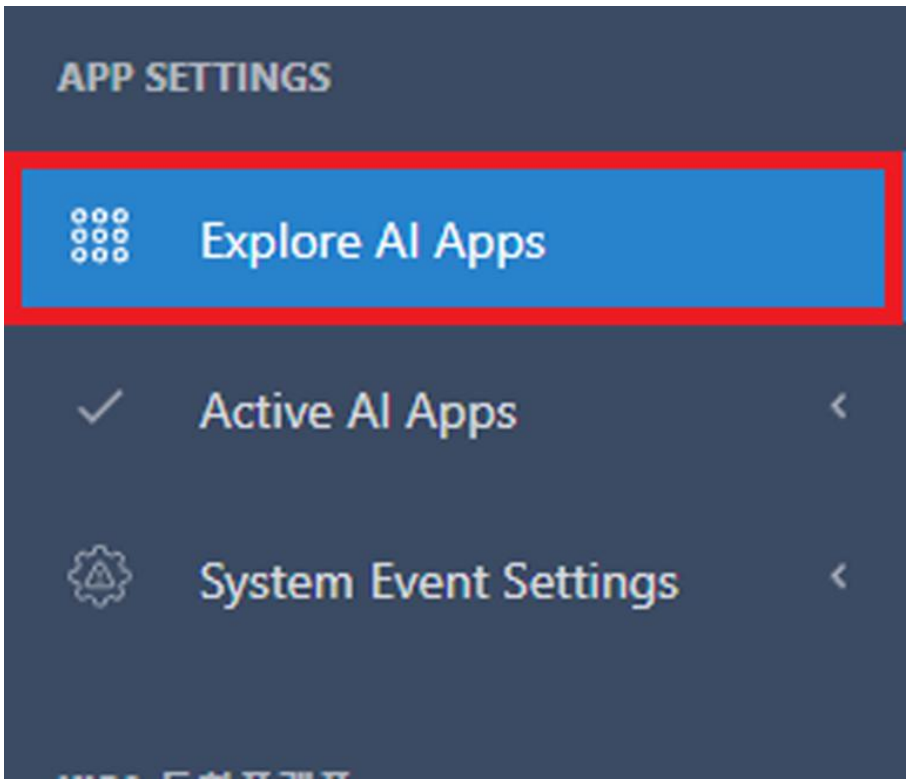


2.3 AIBOX Configuration

2.3.1 Adding AI Apps

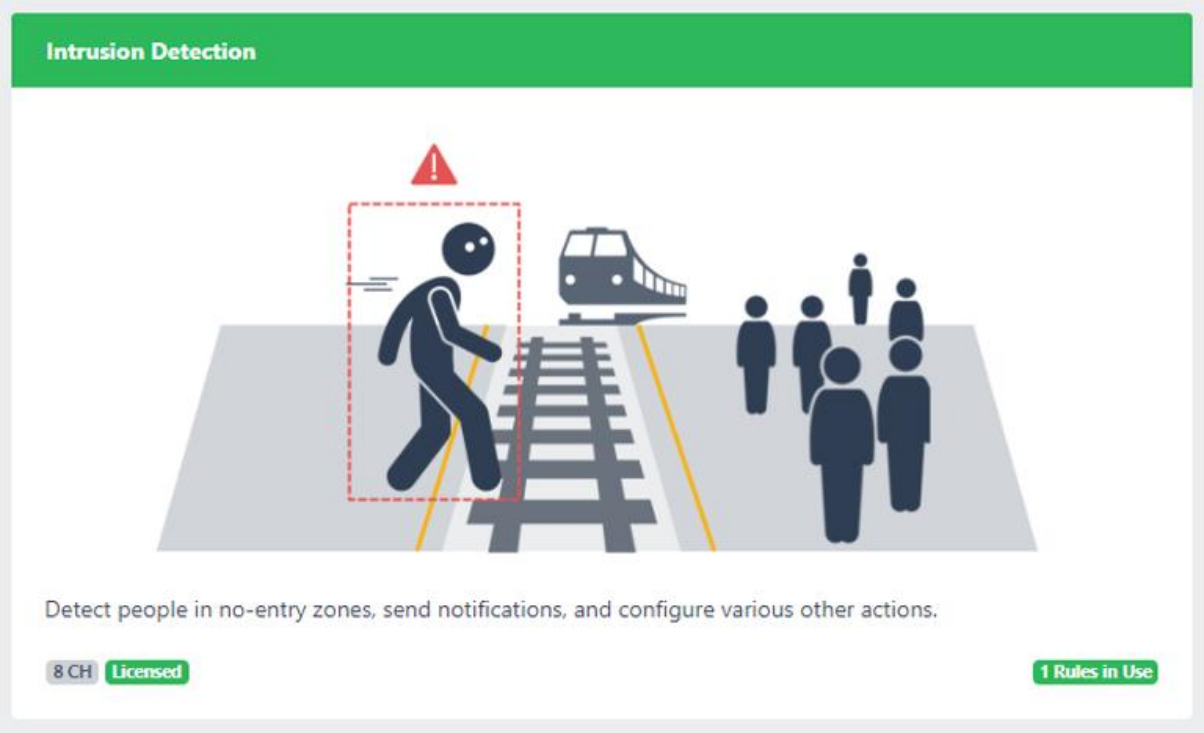
This is a section for creating AIBOX events.

Navigate to: APP SETTING > Explore AI Apps in the menu bar on the left.

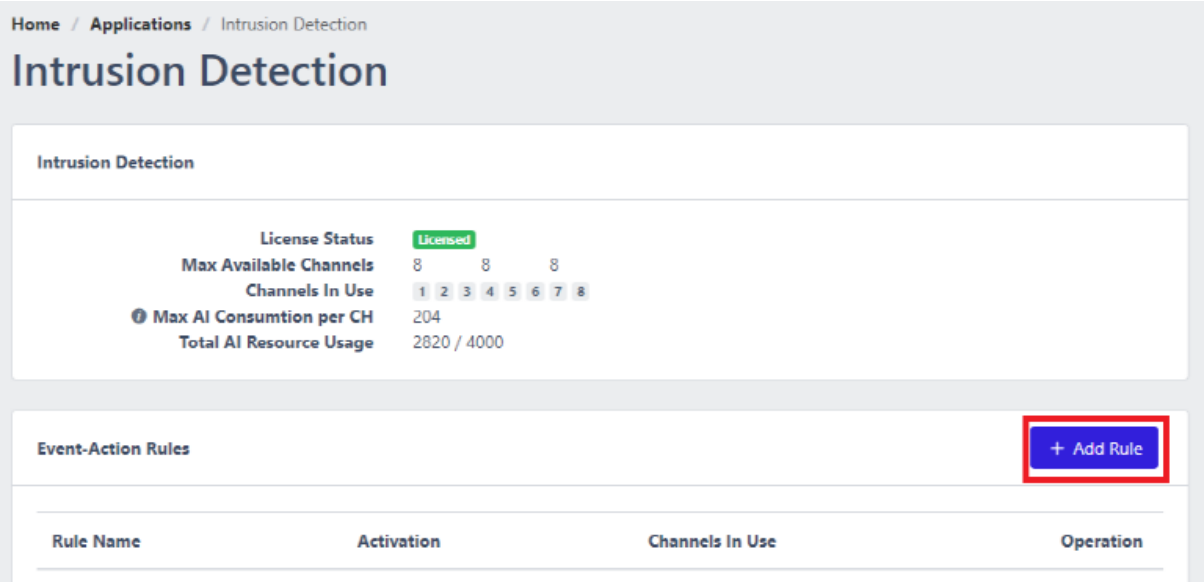


Select the desired AI feature from the available options.

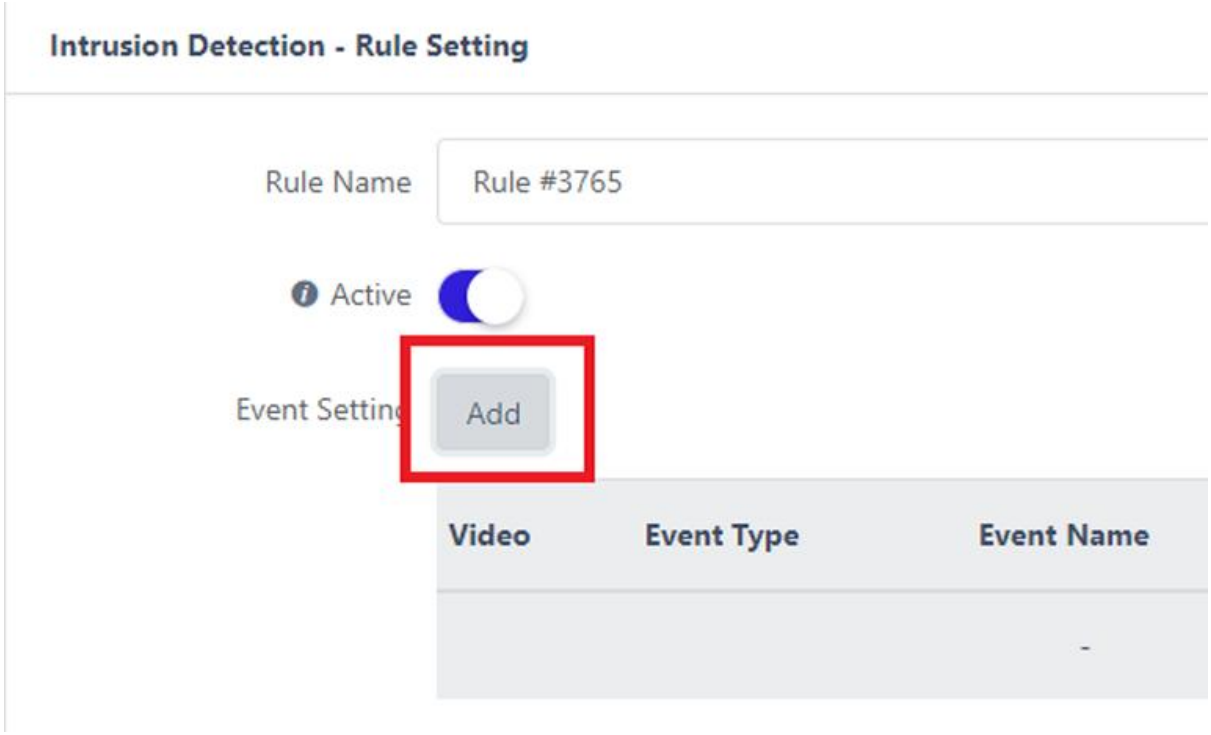
Note : As an example, Intrusion Detection.

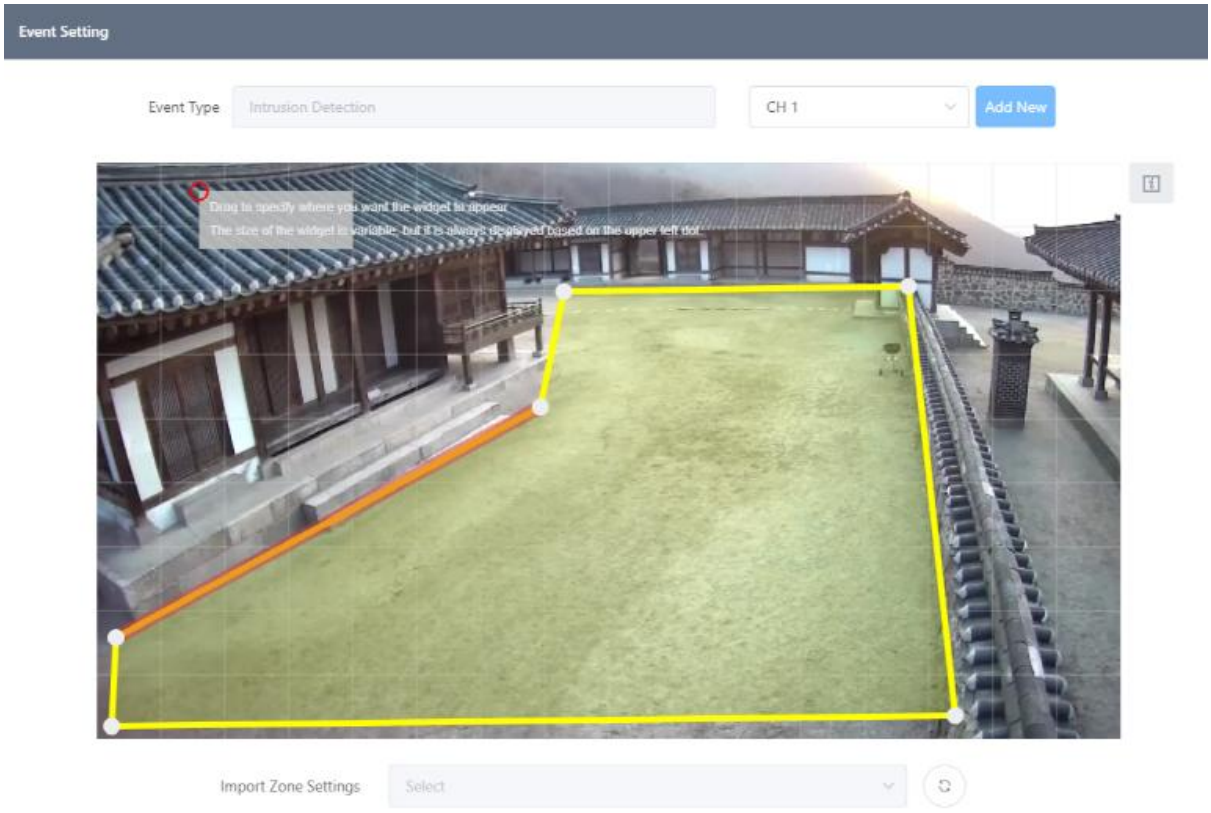


Click ‘Add Rule’.



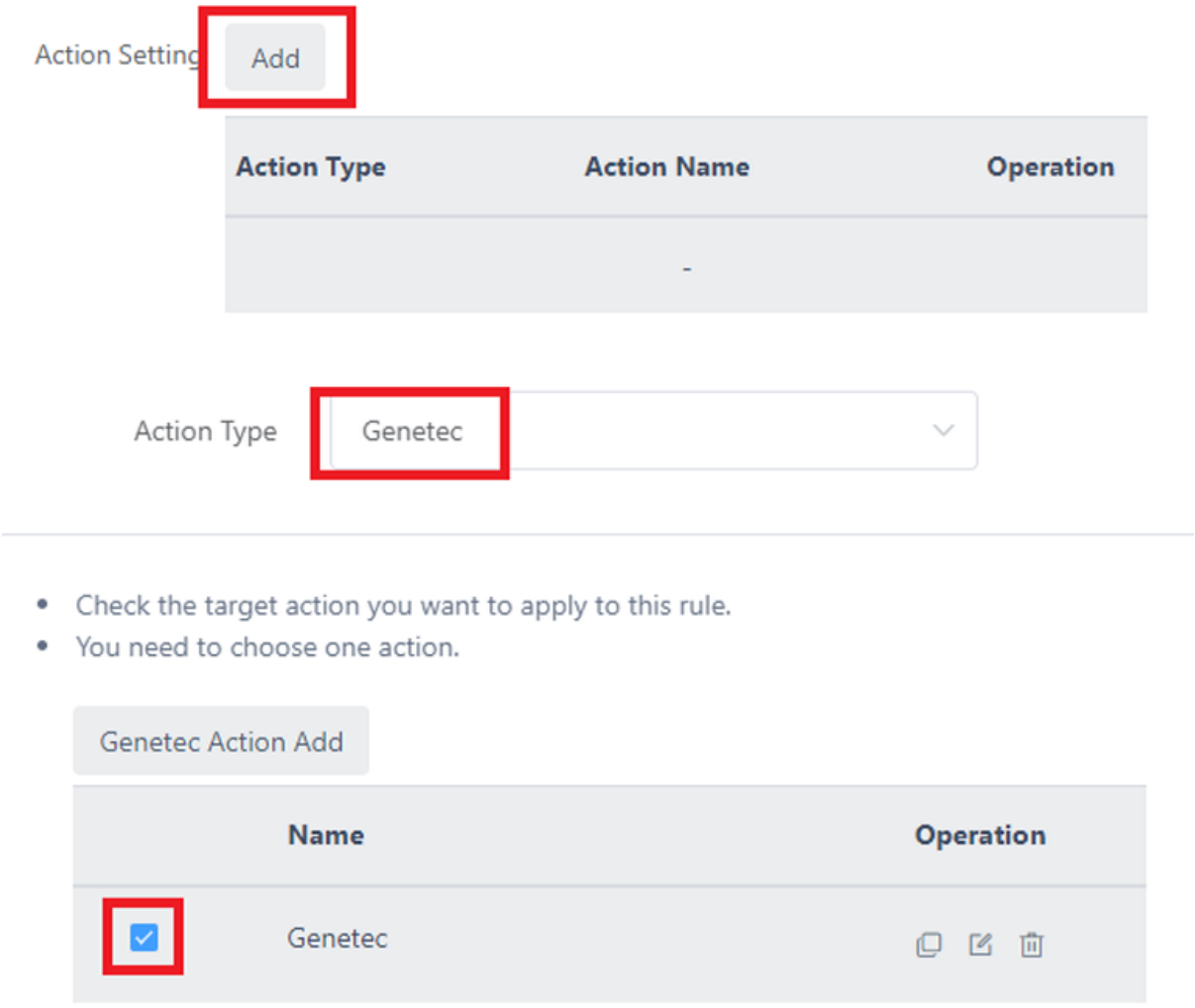
Add Event Setting, set the area, and click Apply.



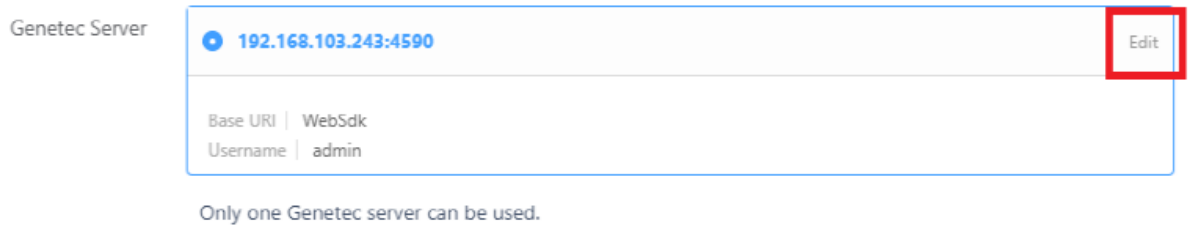


2.3.1 Action Handler Settings

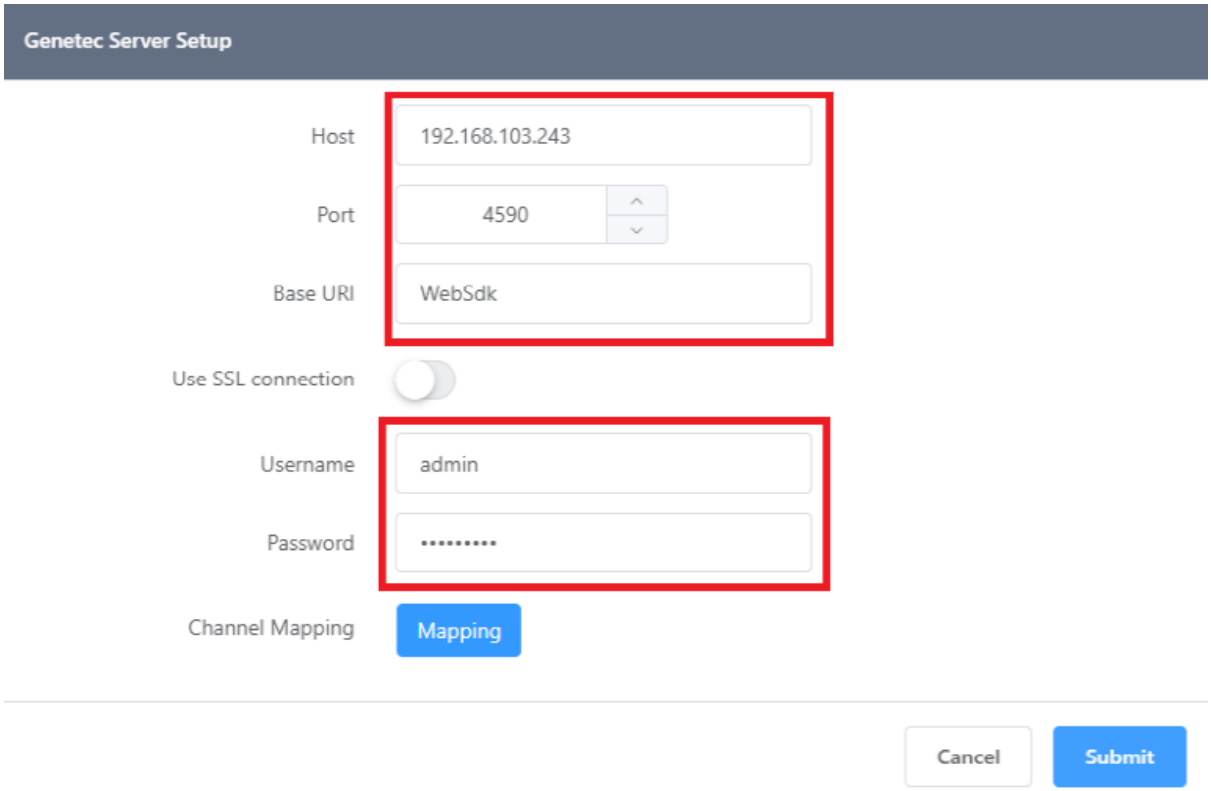
Add Action Setting, select Genetec as the Action Type and check the box.



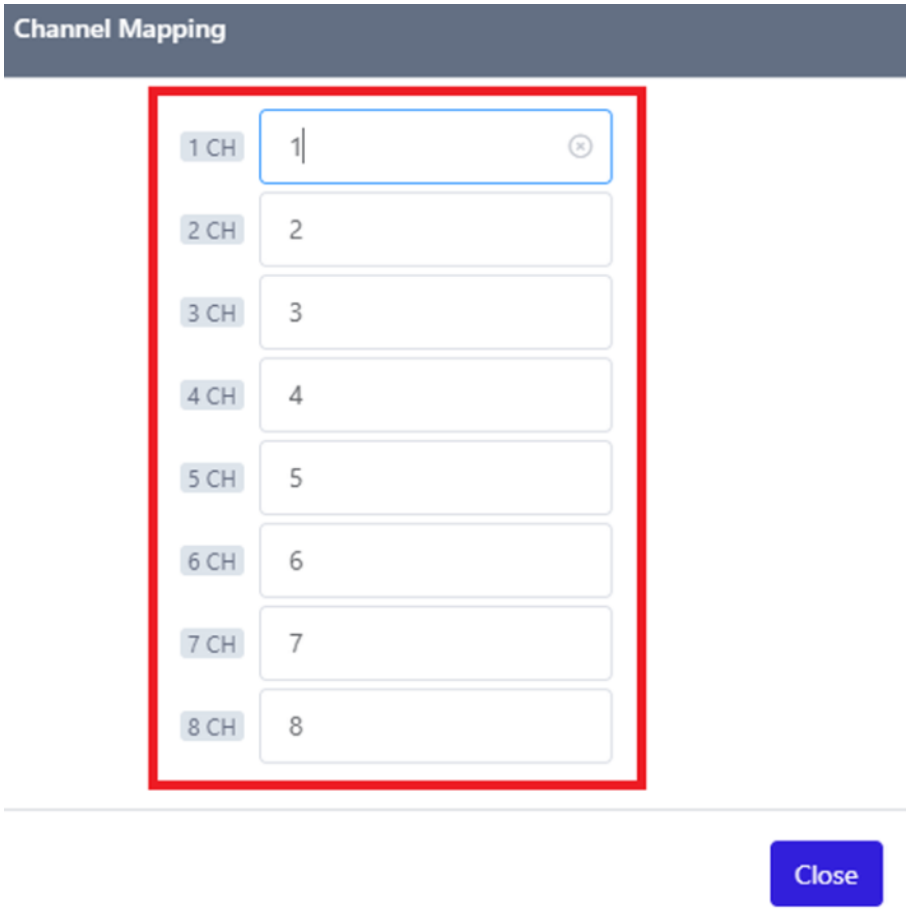
Modify Genetec Server settings:



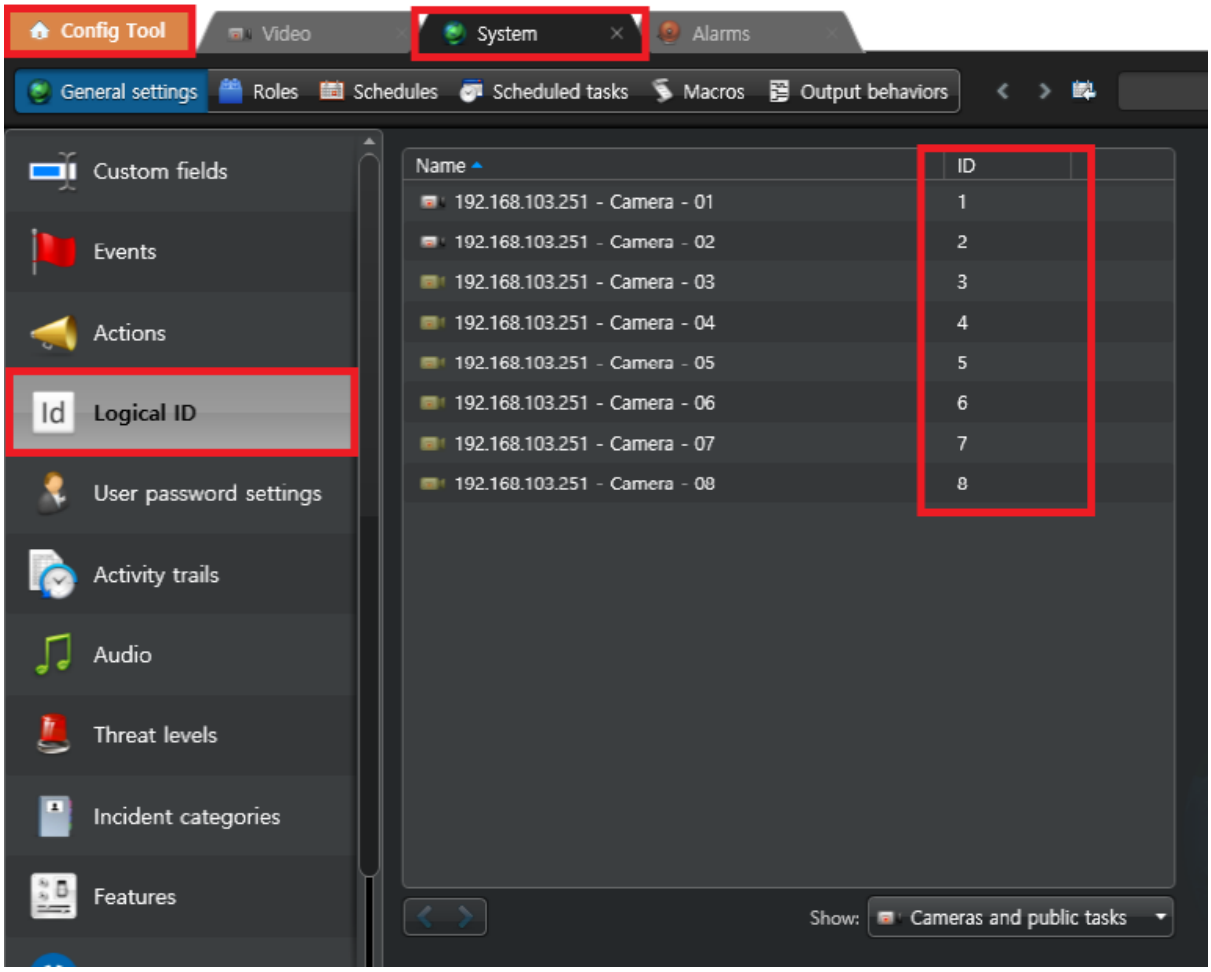
Set the IP of the Genetec Server as the Host, enter the previously set Port number, and set Base URI to WebSDK. Input the ID and password for Genetec.



For channel mapping, click the following button and enter the appropriate Genetec VMS Camera's Logical ID for the corresponding AIBOX's video channel.



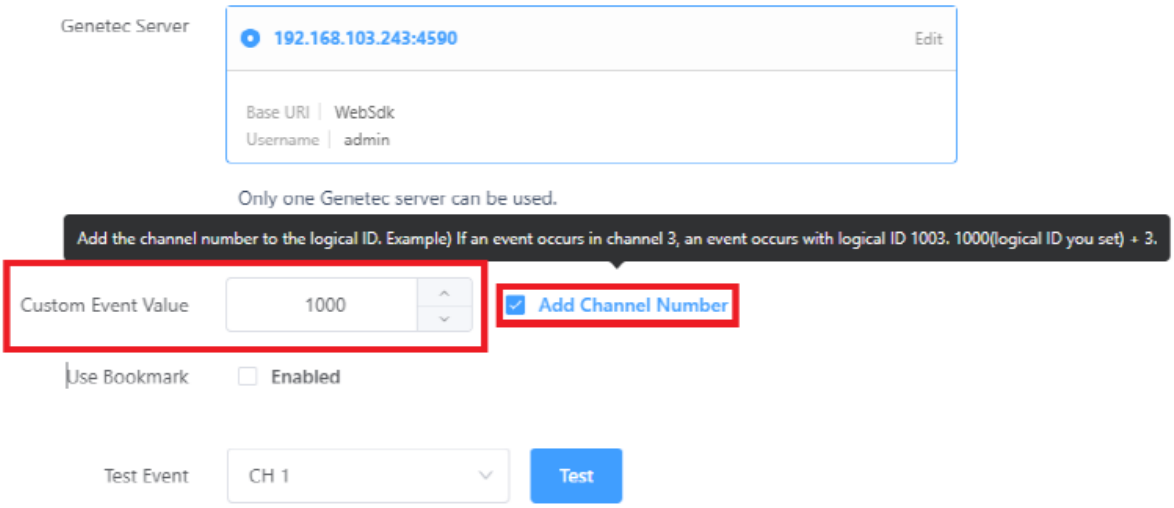
You can check the Channel Logical ID on the Logical ID screen in the Config Tool.

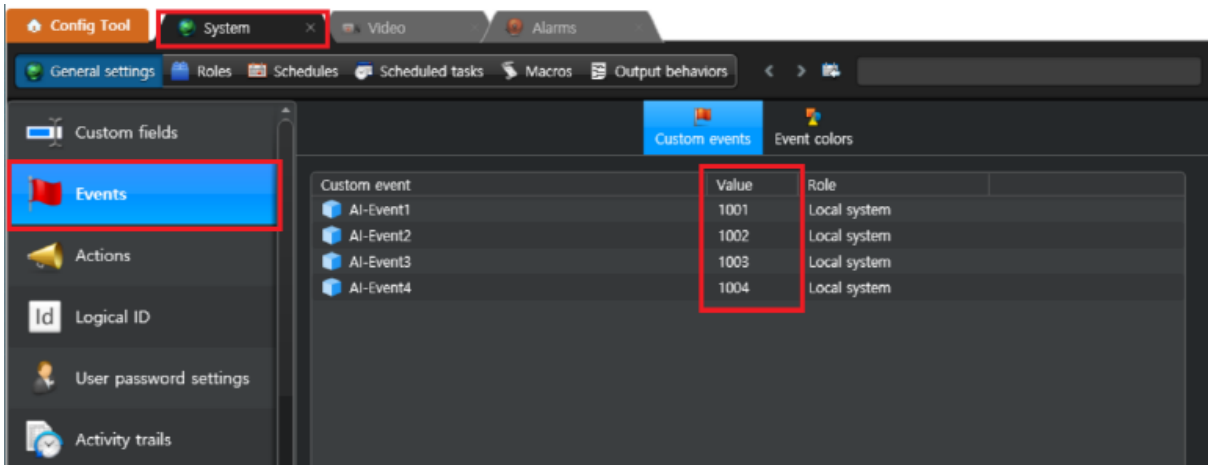


You should enter the **Custom Event Value** created in section 2.2.2, and it can be verified in the Events section of the Genetec Config Tool's System.

If you select '**Add Channel Number**,' the channel number will be automatically added to the Custom Event Value.

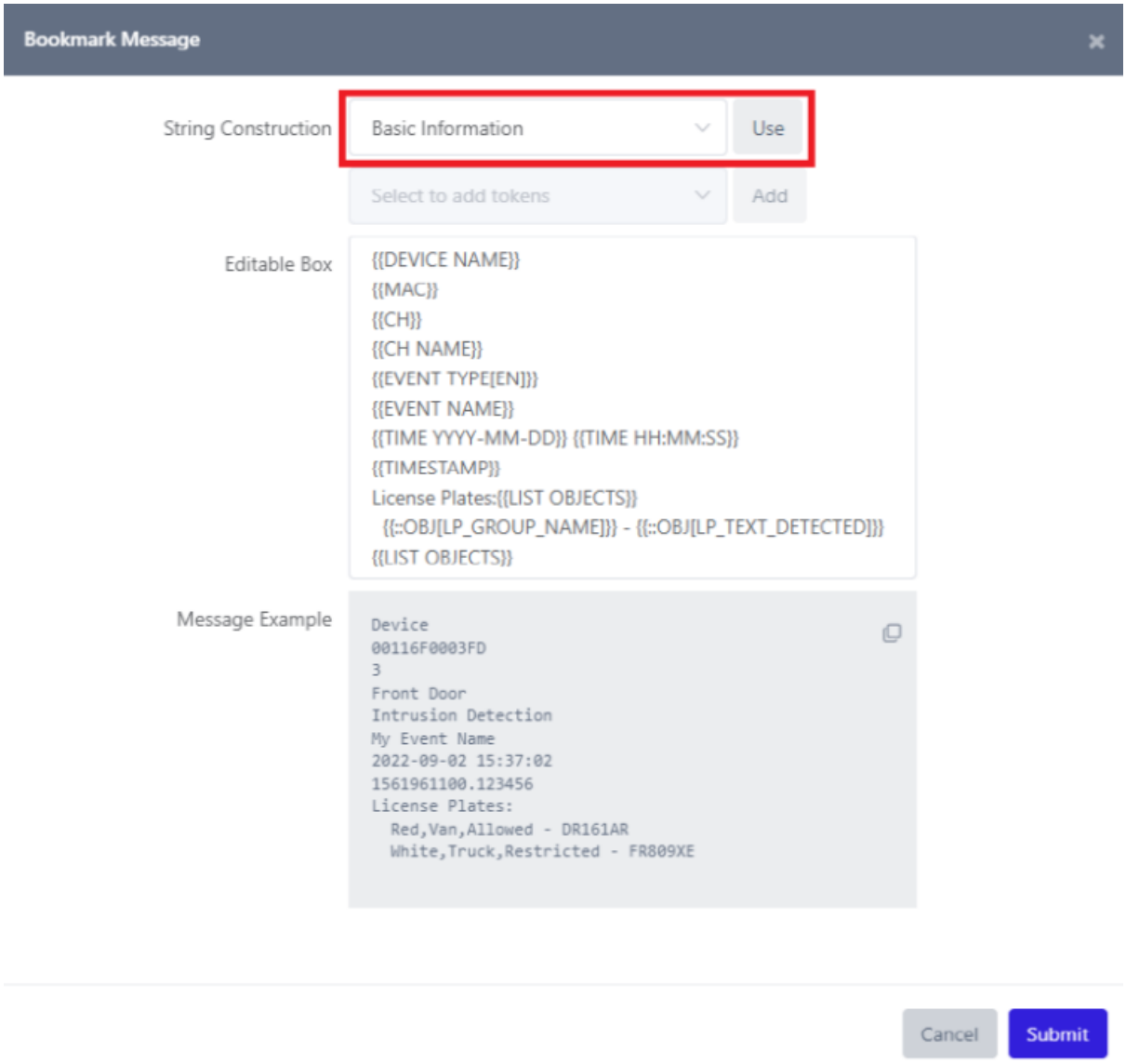
(ex. Channel 1: **1001**, Channel 2: **1002**, Channel 8: **1008)**





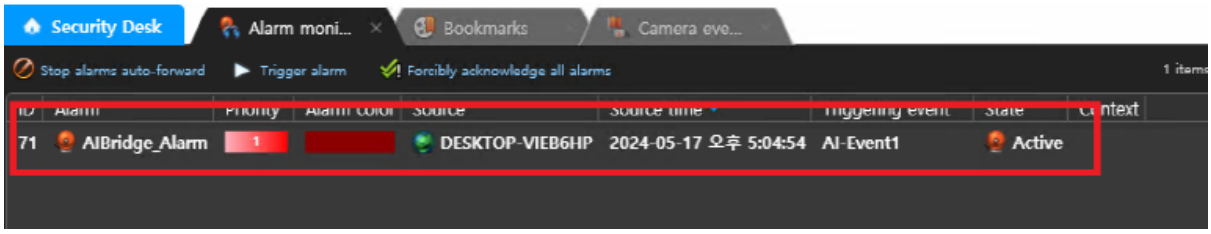
If you want to automatically create bookmarks, select the 'Use Bookmark' option. You can record information such as LPR data or object attributes with the bookmark, and they can be viewed and searched in the Bookmark menu of Genetec Security Desk

Note: For license plate recognition, Basic Notification + LPR is convenient.



Once all settings are complete, you can use the **Test** button to verify if the event integration is working properly.

If the event is successfully transmitted, an alarm will appear in Alarm Monitoring.

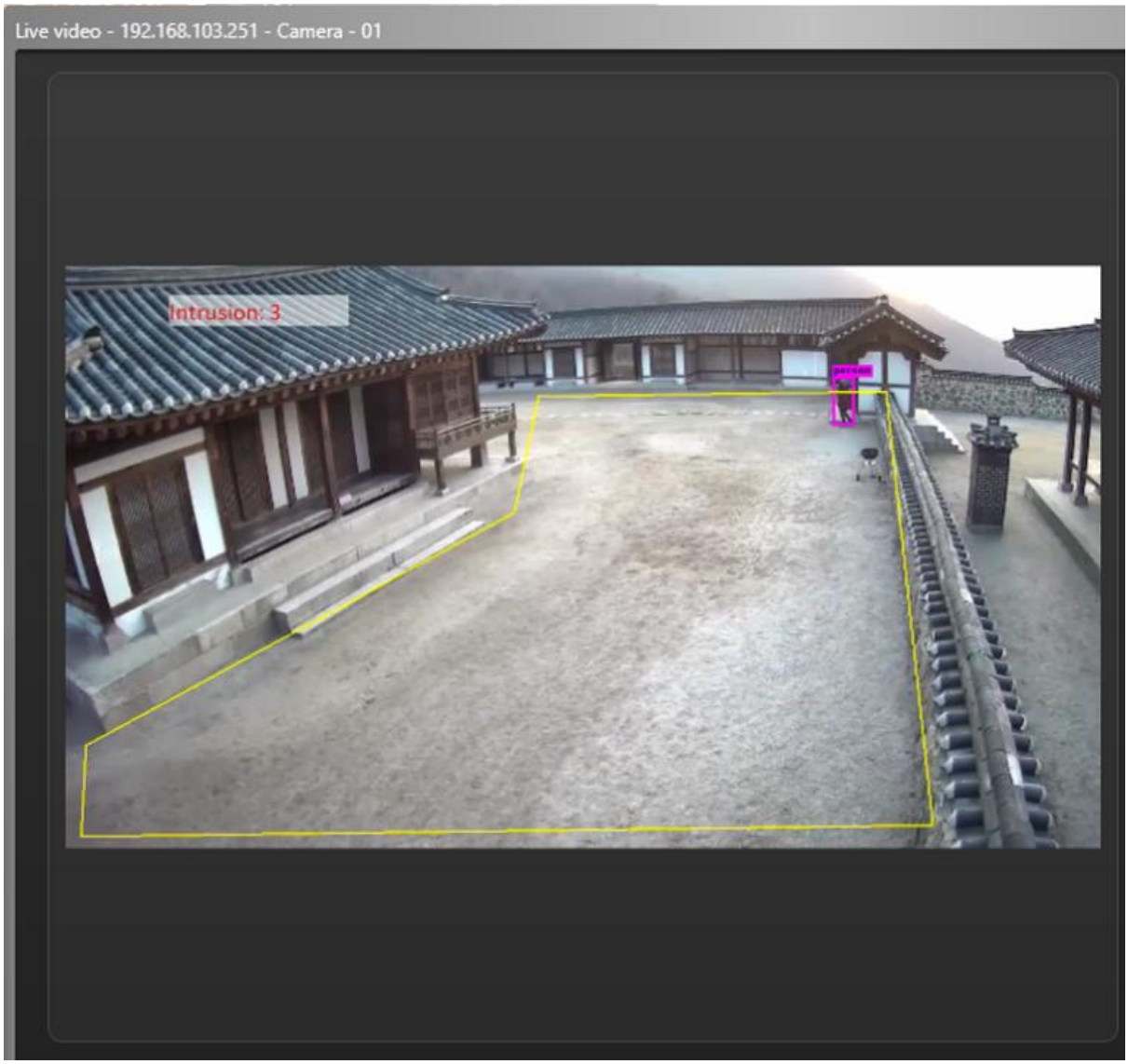


Tip : If the event is not working properly, check the firewall.

3. Demo

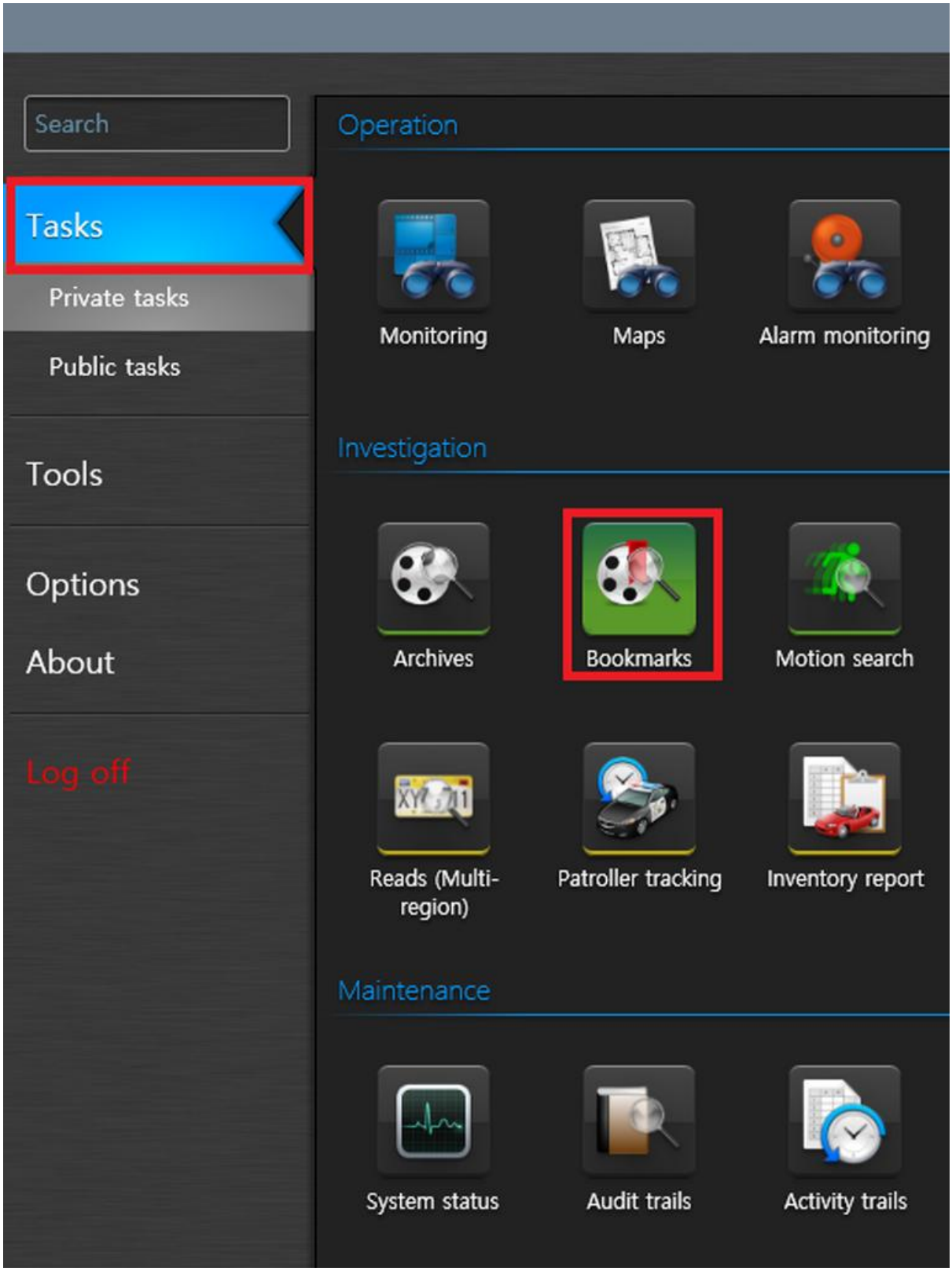
3.1 Live

In the Video tab of the Config Tool, you can check the Live Video.

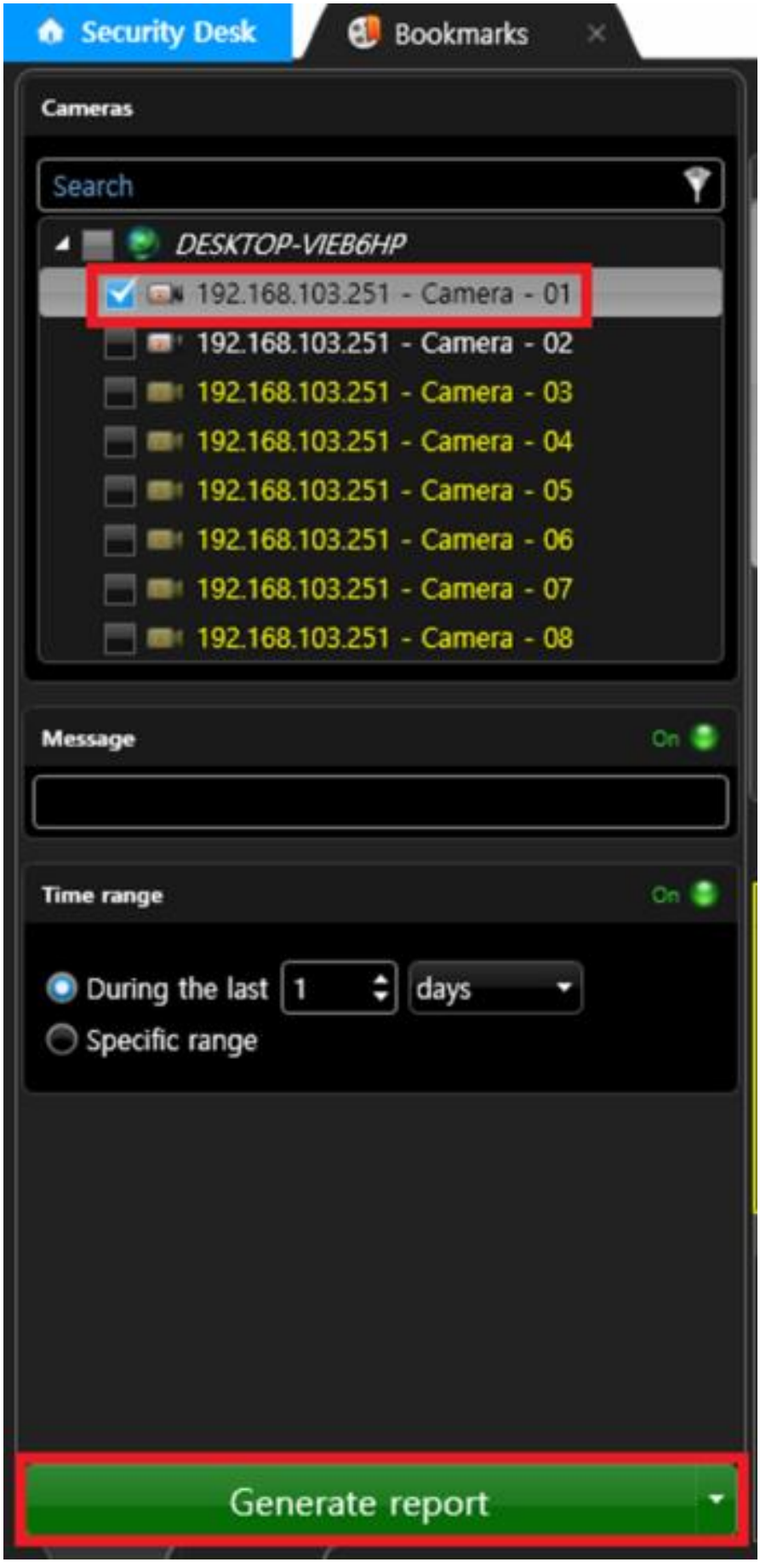


3.2 Bookmark

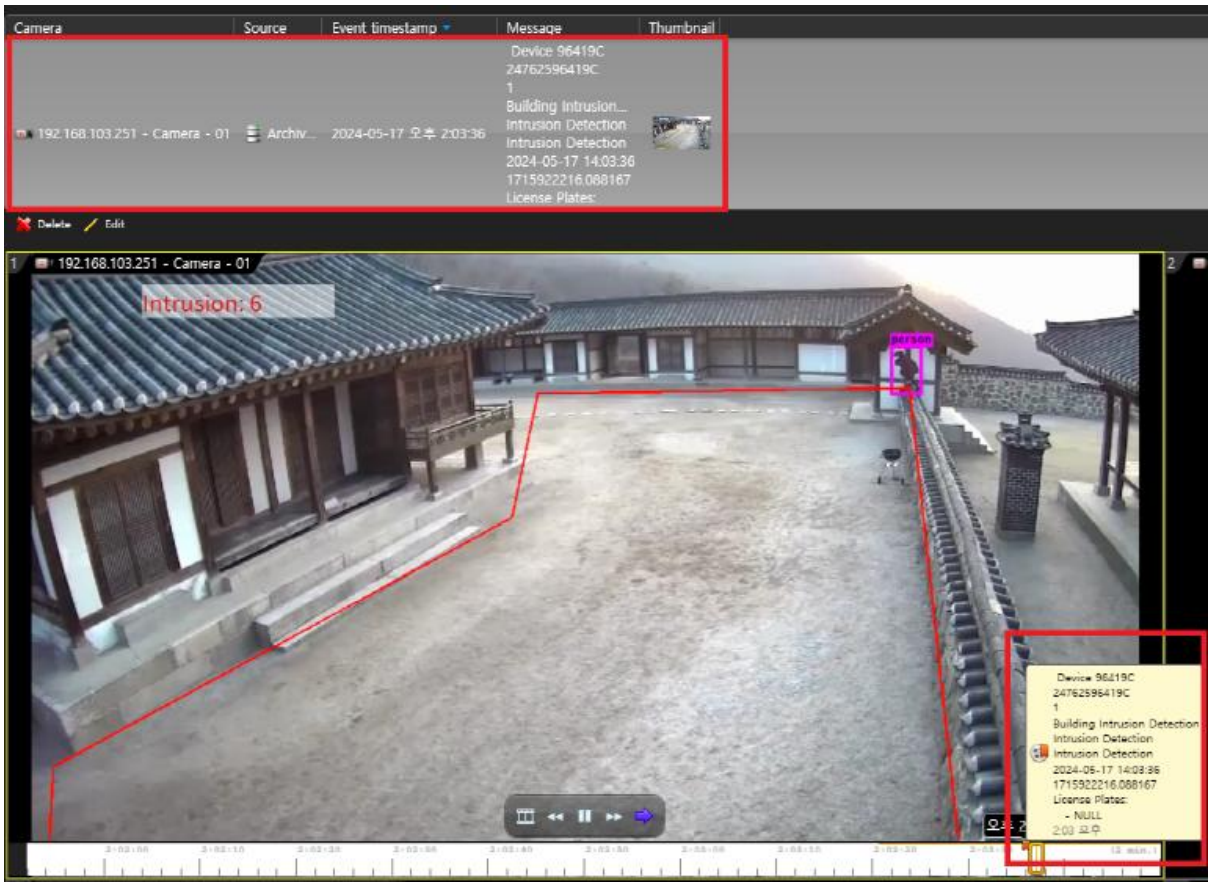
Navigate through: Genetec Security Desk > Task > Bookmarks



Select the desired camera and then click the report button.Note:Events do not update in real-time, so it is necessary to click the report button to refresh.


Security Desk
Bookmarks
Cameras
Search
DESKTOP-VIEB6HP
192.168.103.251 - Camera - 01
192.168.103.251 - Camera - 02
192.168.103.251 - Camera - 03
192.168.103.251 - Camera - 04
192.168.103.251 - Camera - 05
192.168.103.251 - Camera - 06
192.168.103.251 - Camera - 07
192.168.103.251 - Camera - 08
Message
On
Time range
On
During the last
1
days
Specific range
Generate report

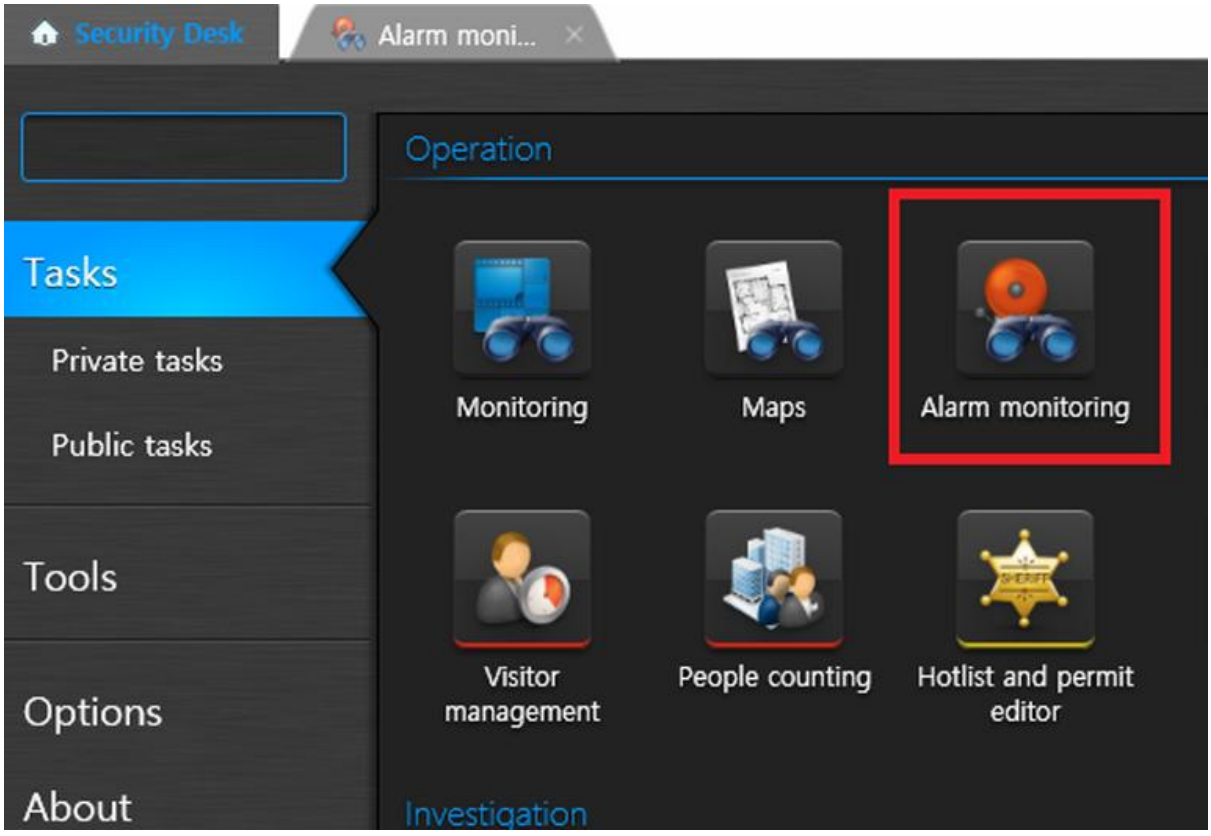
View the bookmarks and videos related to the occurred events.



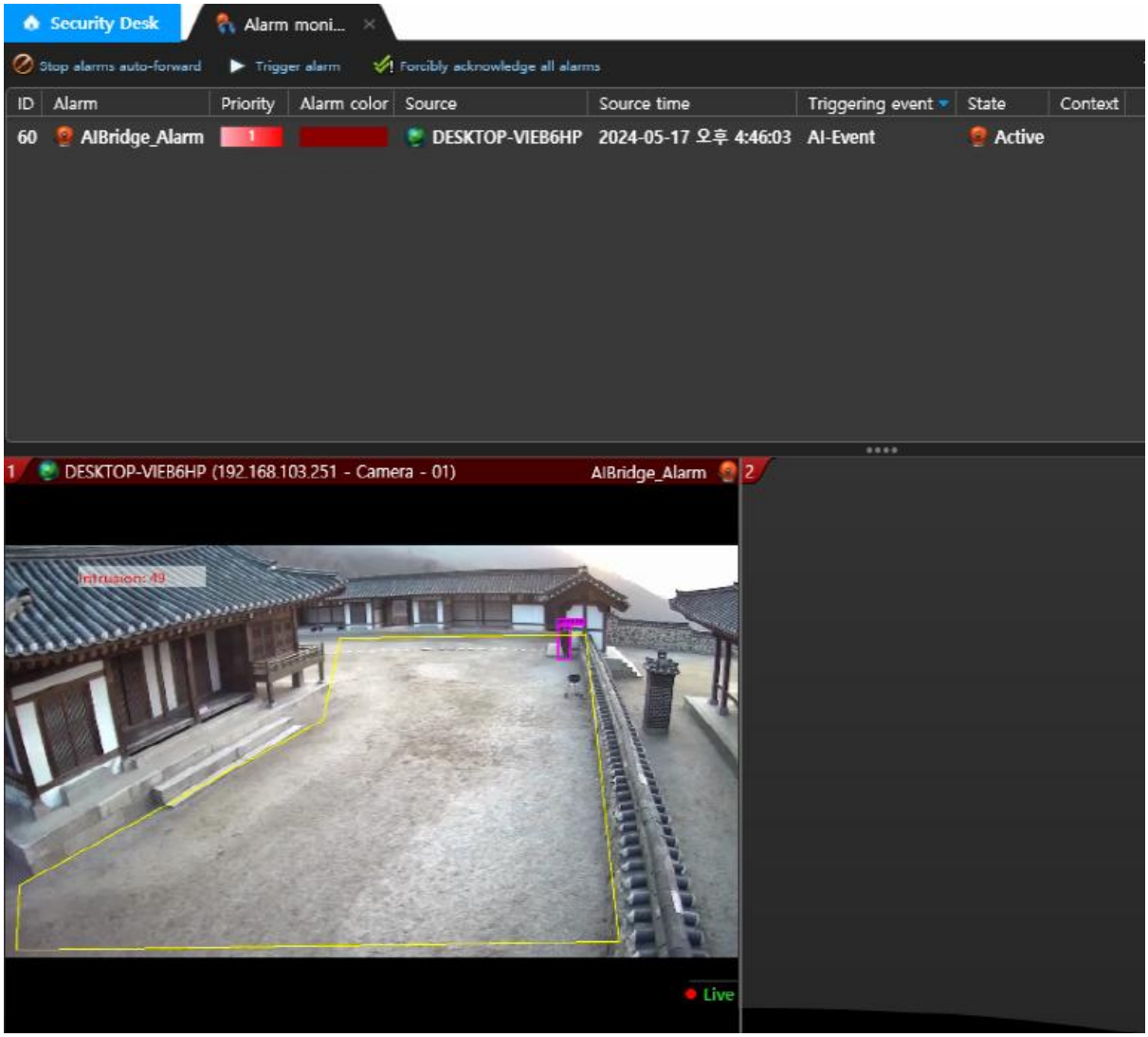
3.3 Alarm Monitoring

You can Alarm Monitoring in real time.

Select the Alarm Monitoring menu in Security Desk. You can then view real-time alarm monitoring information for events with real-time alarm triggers, as configured in section 2.2.3.



When a real-time event occurs, you can manage the alarm while viewing the associated alarm event and the related video channel.



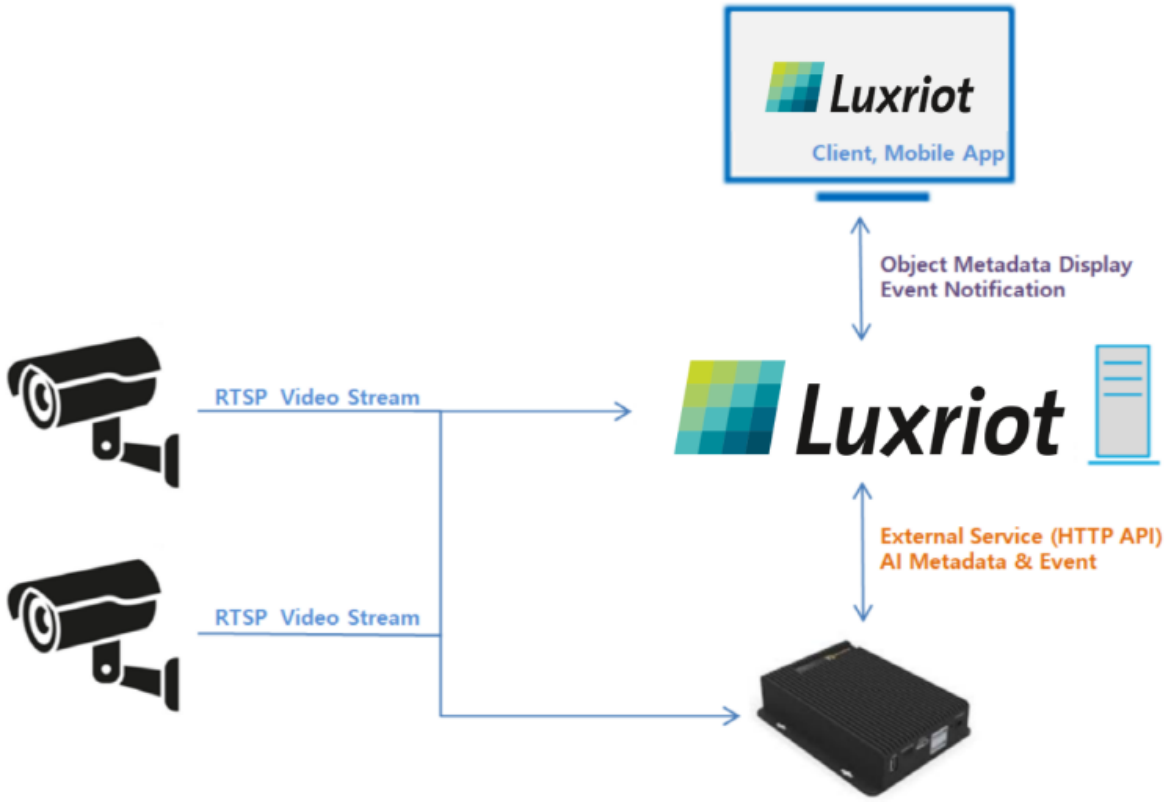
Luxriot Evo Integration Guide

1. Introduction

1.1 Prerequisites

- AIBOX FW version 103808 or greater.
- Luxriot Evo S/ Global VMS version 1.22 or greater.

1.2 Learn about integration architecture



IP Camera transmits video stream to Luxriot VMS and AIBOX.

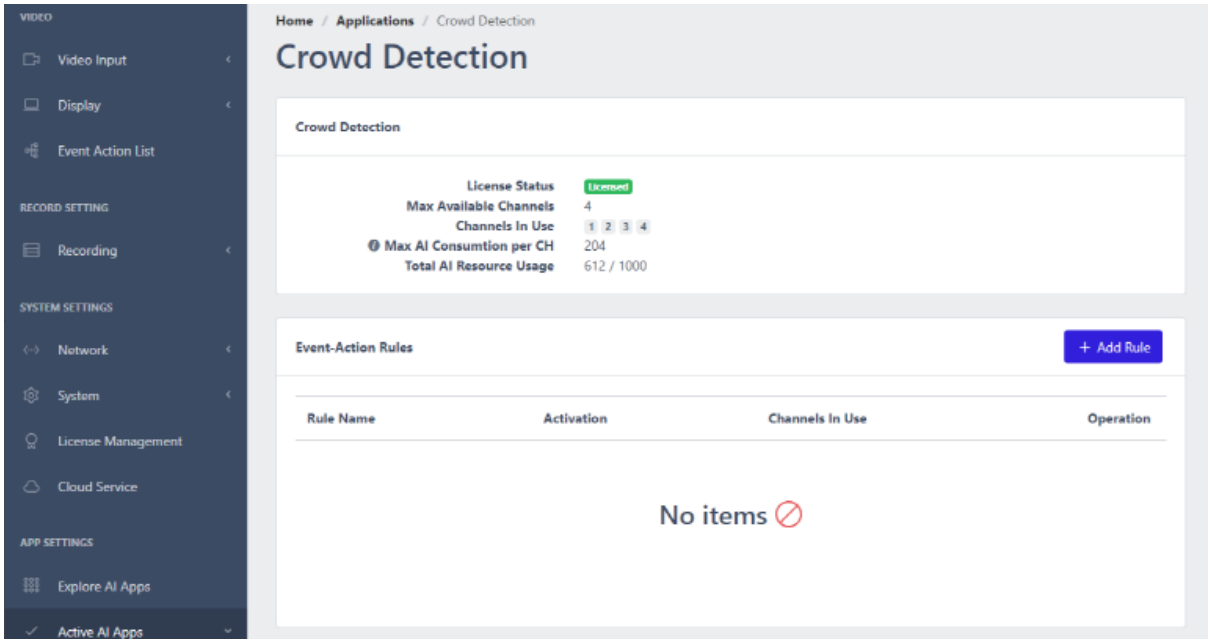
AIBOX analyzes the received video stream by AI Apps and sends metadata & event to Evo VMS.

AIBOX responds to Evo VMS's search requests.

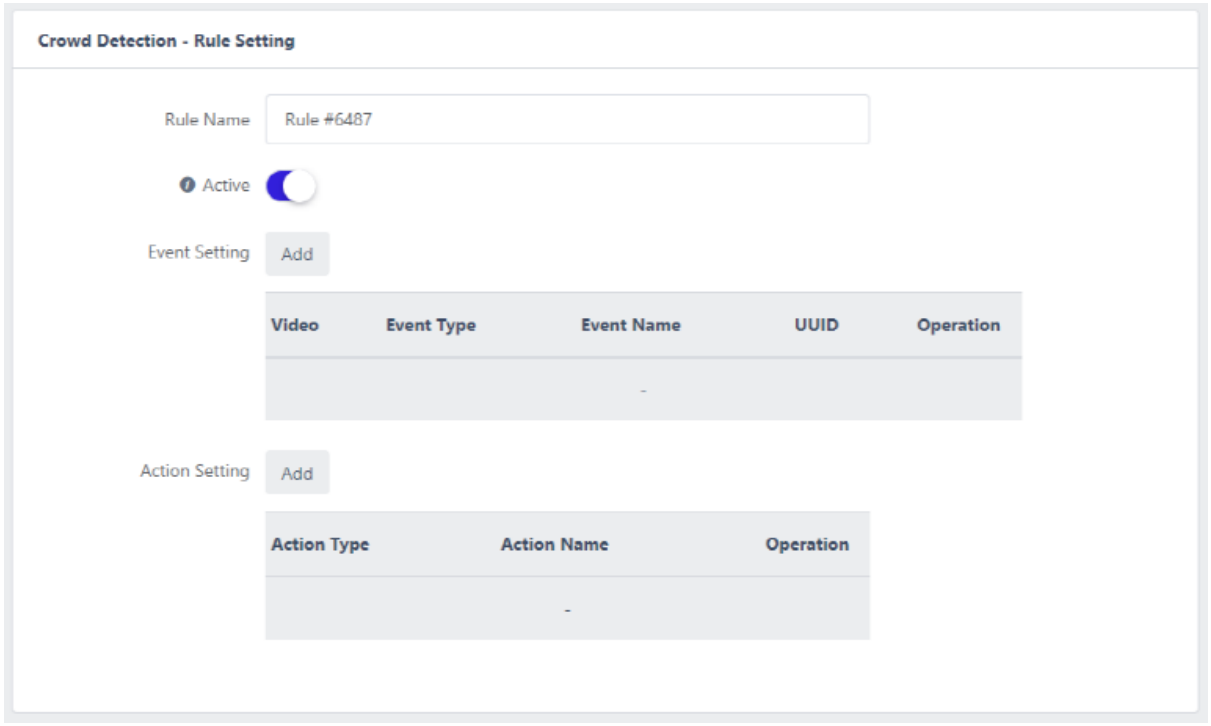
2. Configuration

2.1 AIBOX Configuration

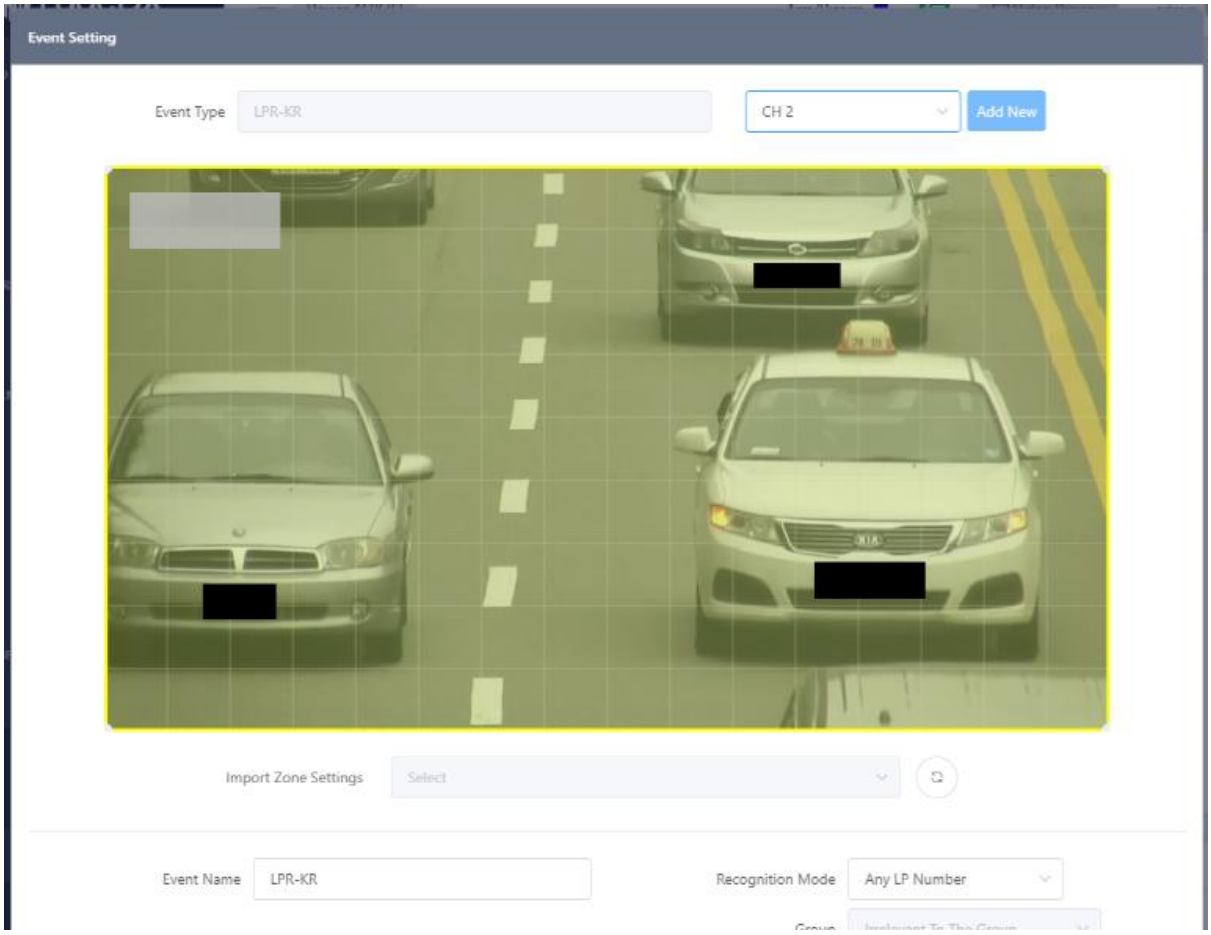
Add AI app settings.



Add Event Setting.

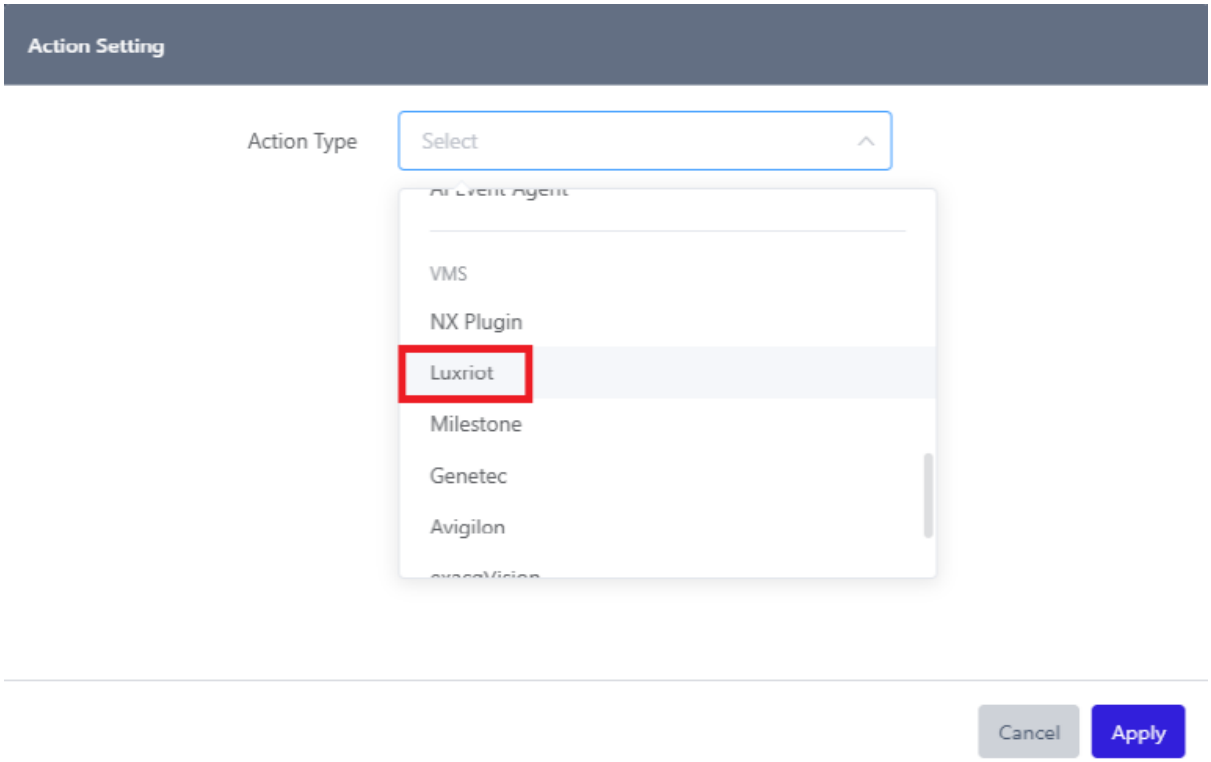


Zone or detailed setting of AI App.

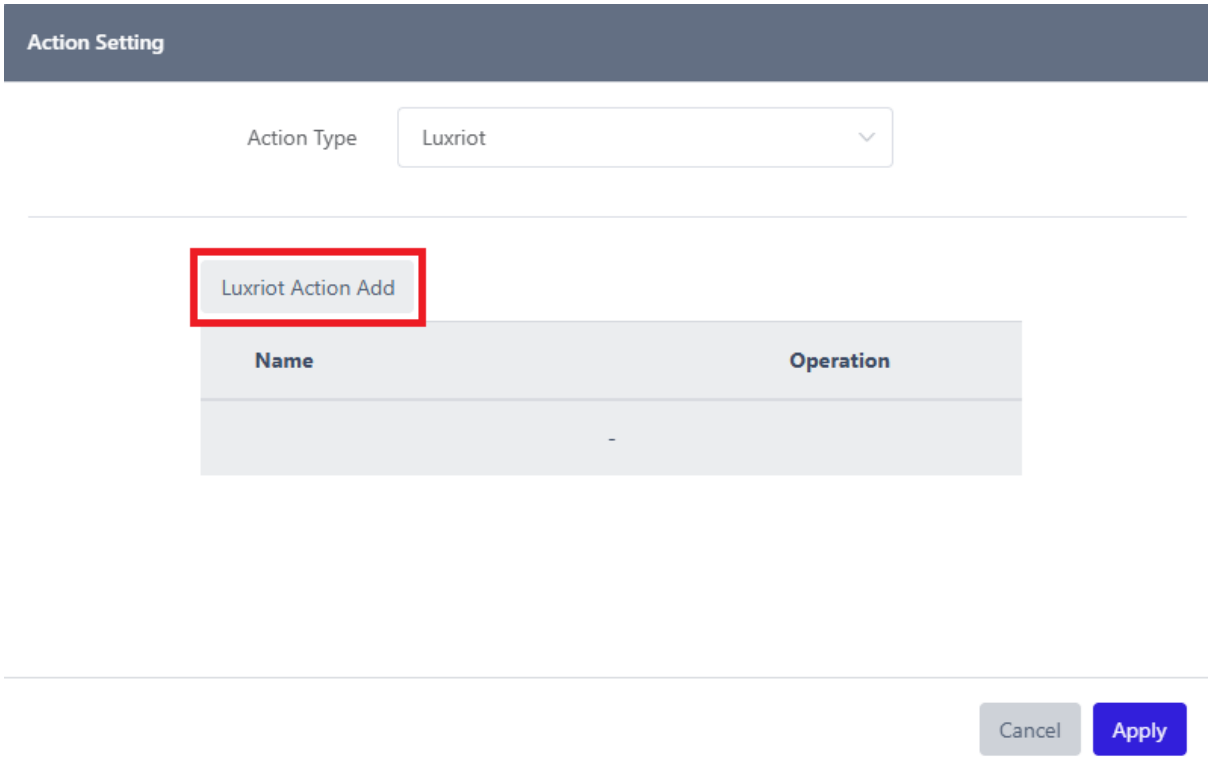


Add Luxriot Plugin Action Setting.

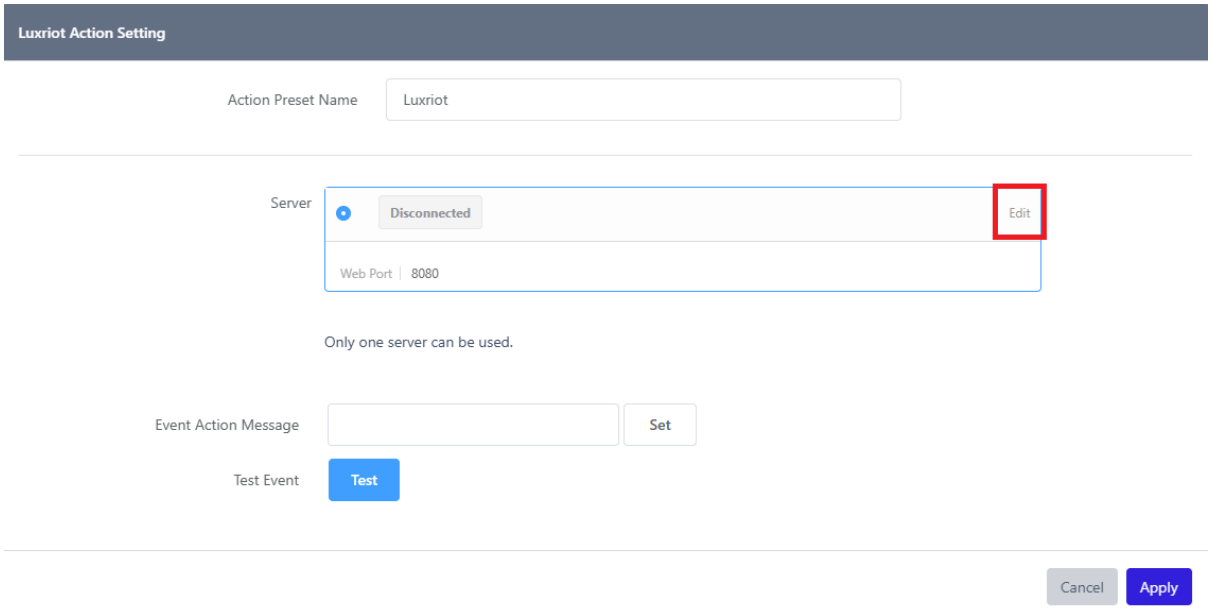
Select Luxriot.



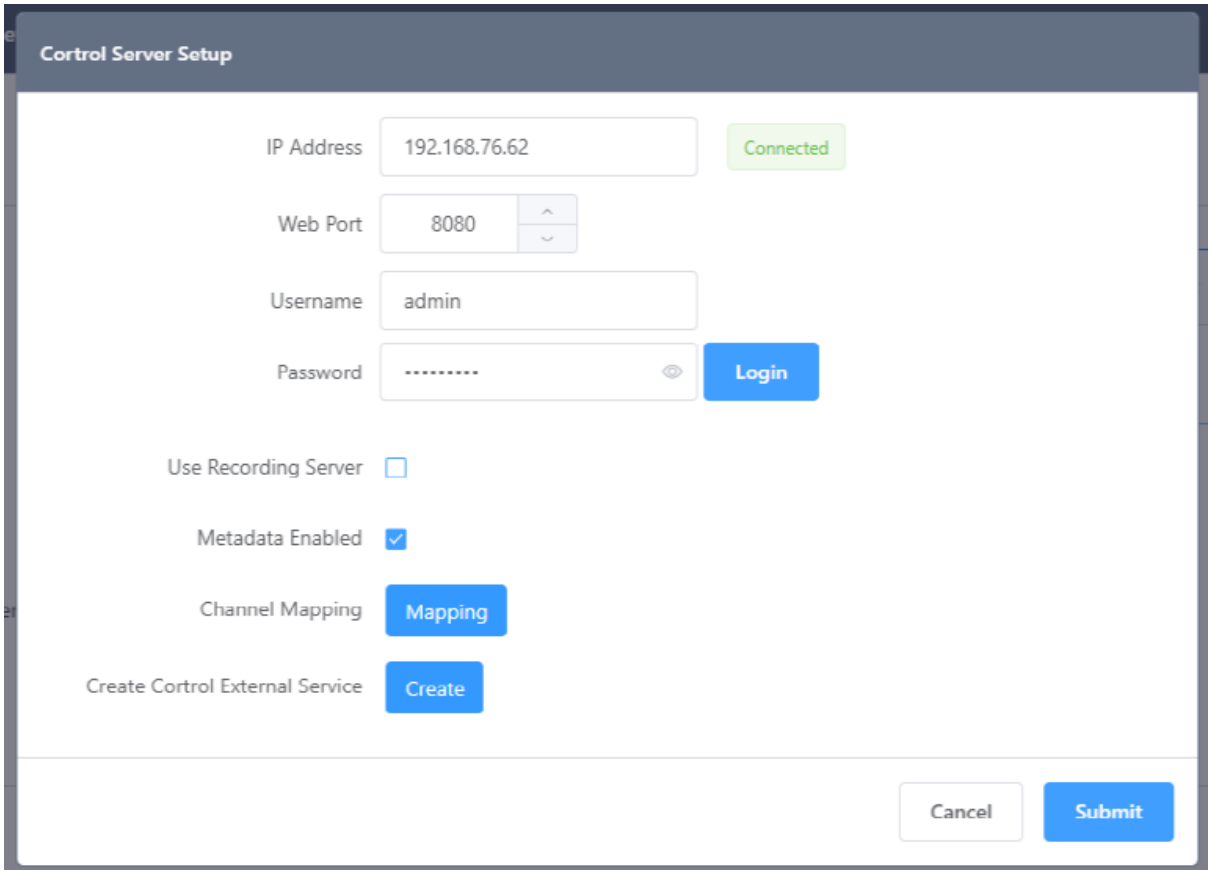
Click the “Luxriot Action Add” button.

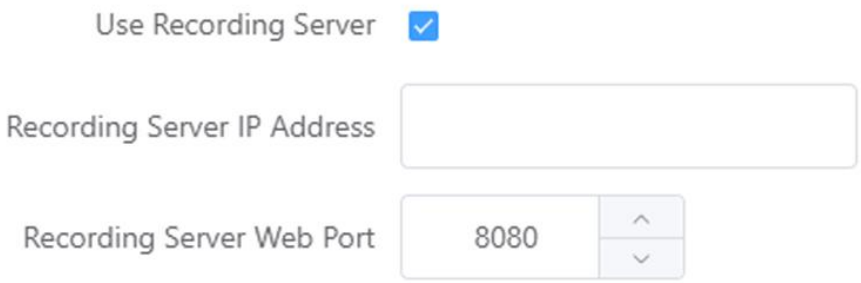


Click the “Edit” button.



Enter the Evo VMS information (Server Address, Port number, Username, Password)
You can check if the Evo VMS settings are correct through the **“Login”** button.





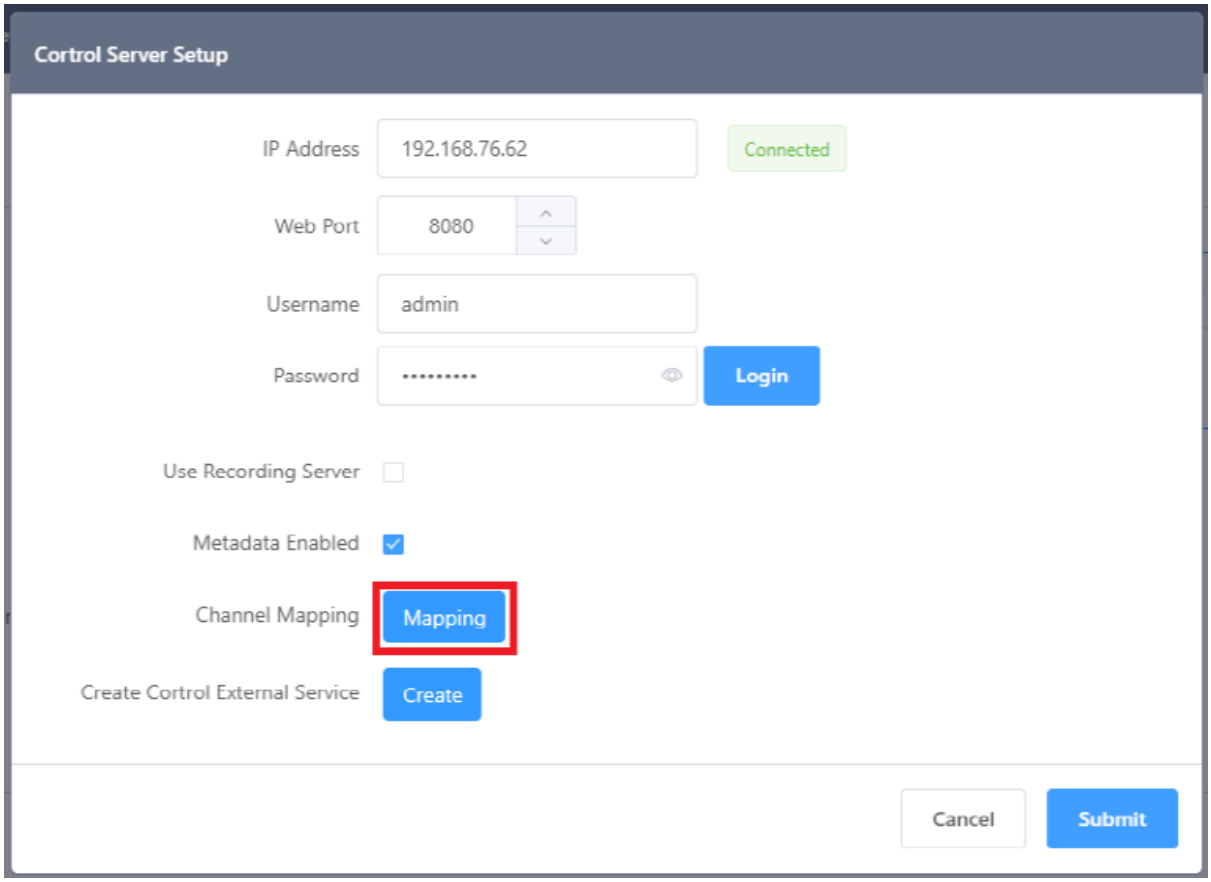
Note. When **"Metadata Enable"** is enabled, AIBOX transmits object Metadata detected by AI to Evo VMS. Please note that performance issues may occur if the AI app is installed in an environment where many objects are detected.

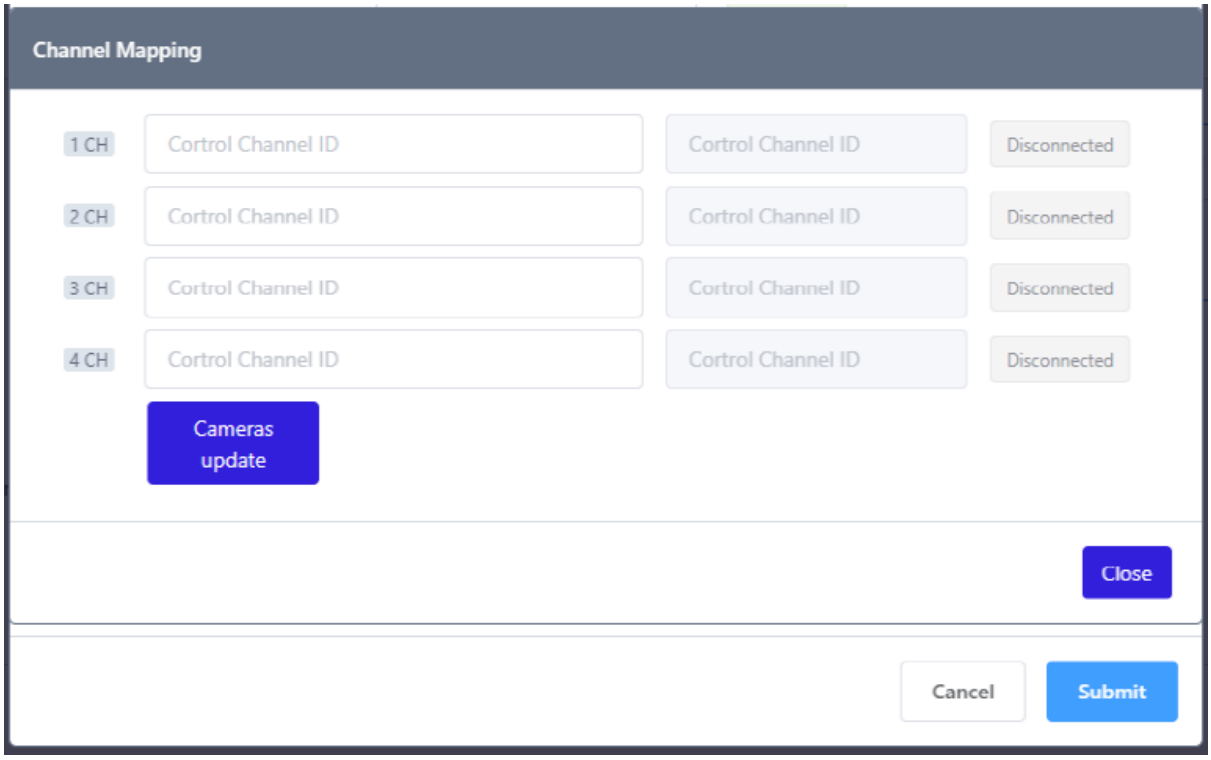
Note. If you are a Luxriot Evo Global user and have registered the device using Evo Recording, please check 'Use Recording Server and enter the ID and password. For the Luxriot Evo S, you do not need to check this option.

2.2 AIBOX Channel Mapping

Set up the relationship between the AIBOX channel and the channel of Evo VMS.

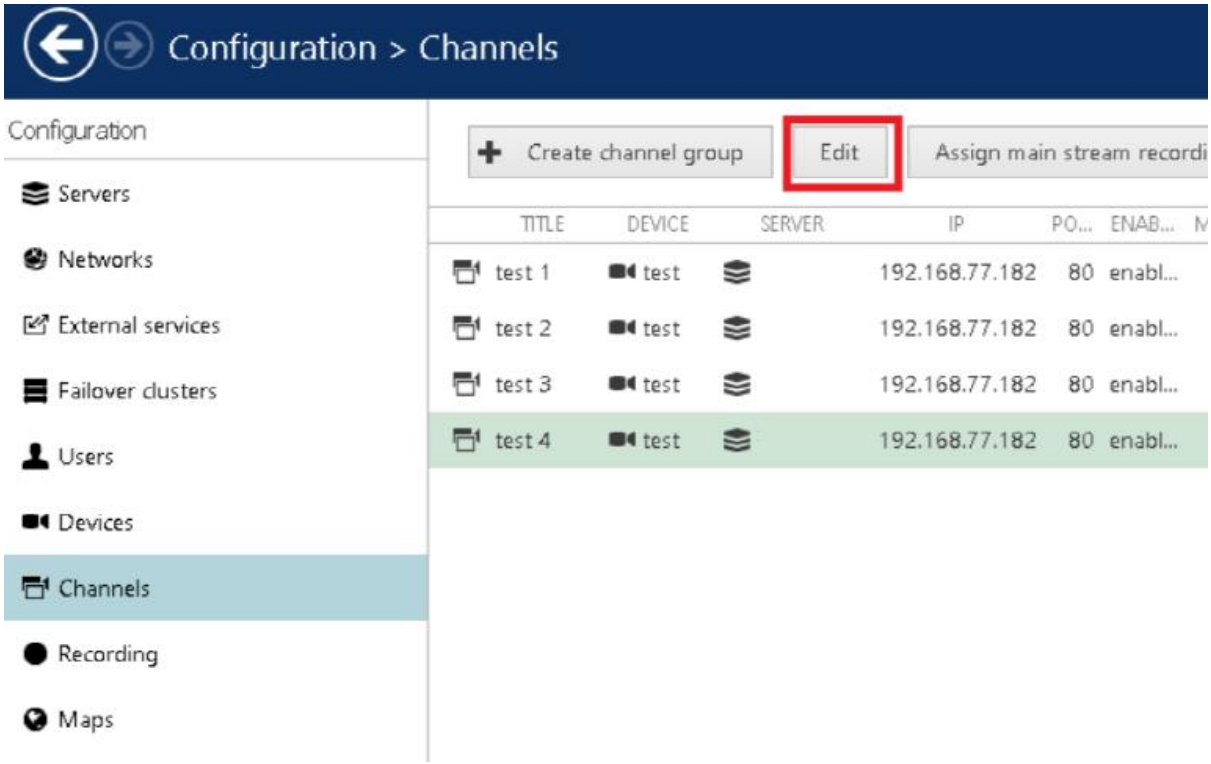
Press the "Mapping" button to open the settings pop-up window.

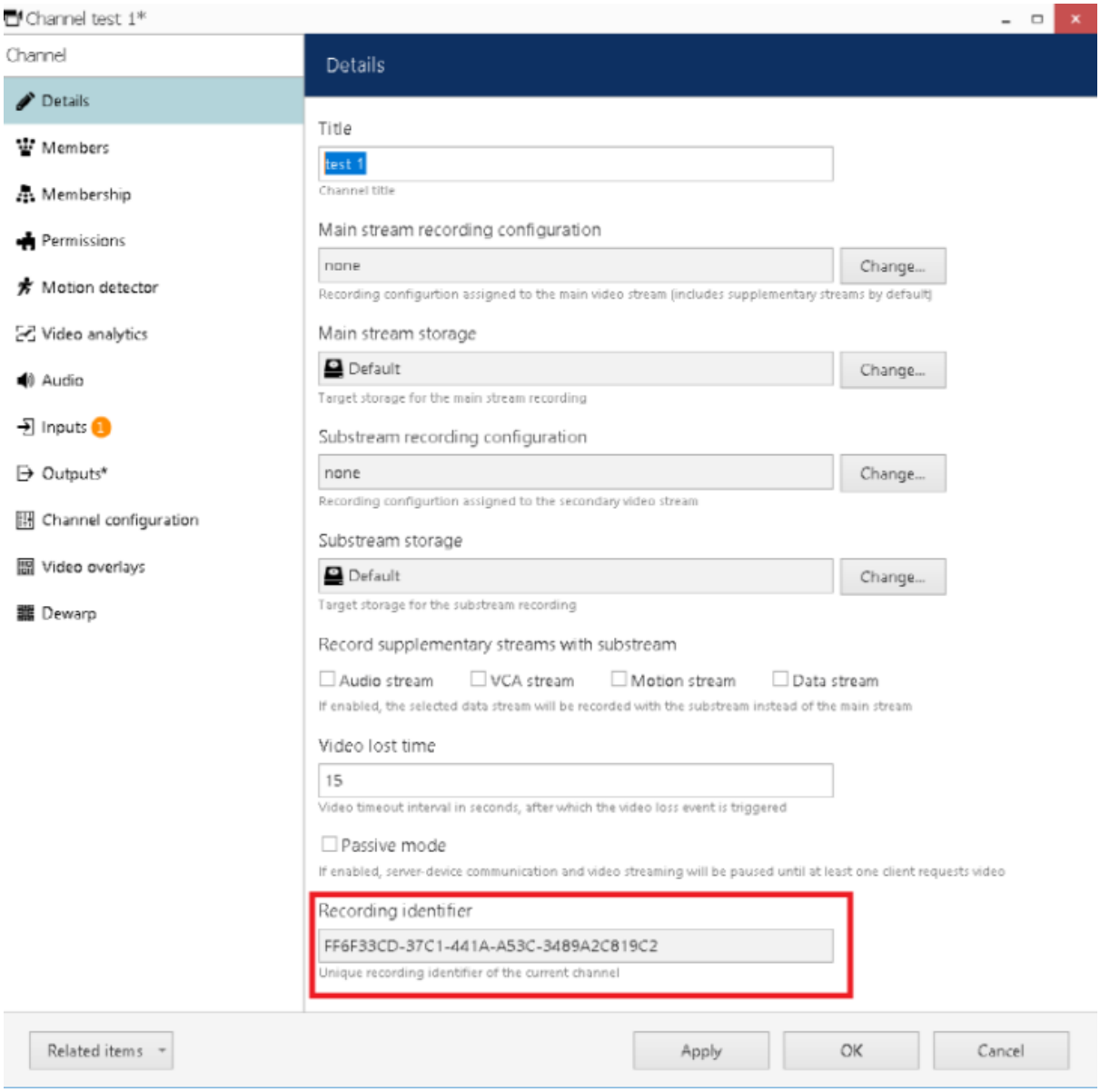


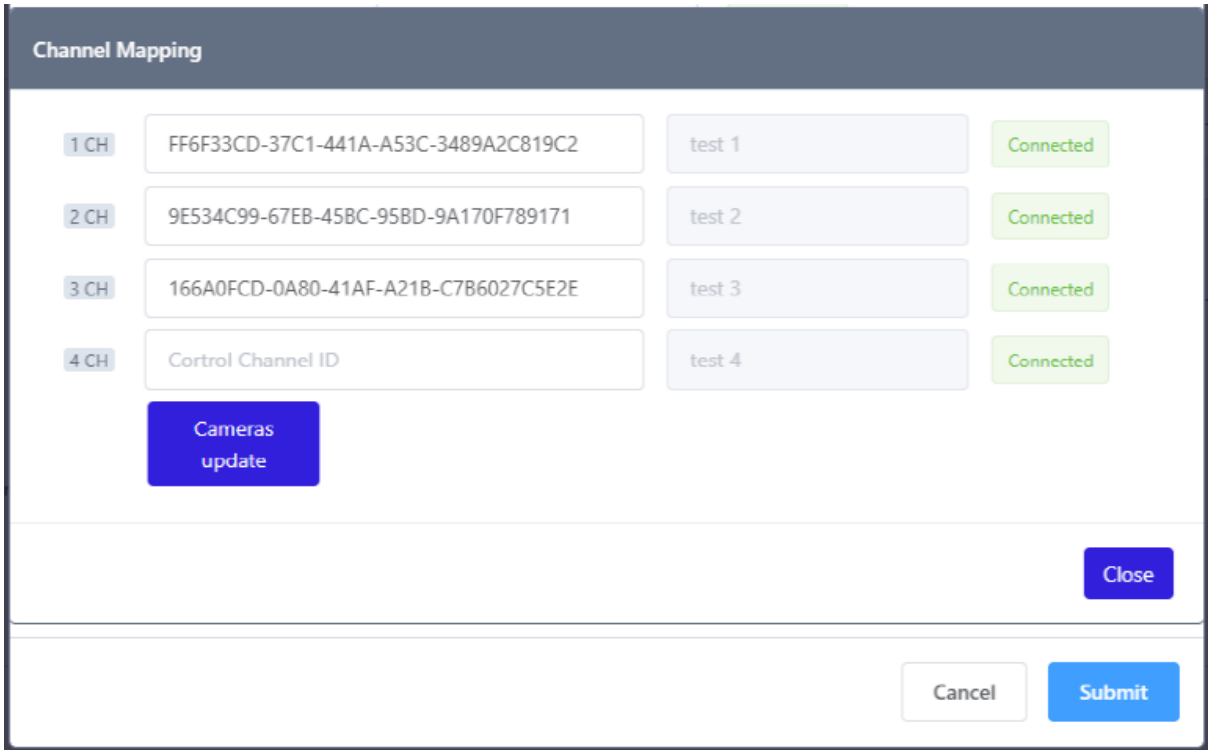


Enter the **Recording identifier (UUID)** of the channel registered in Evo VMS into AIBOX.

Recording identifier (UUID) can be obtained from the Details menu of Channel in Evo Management Console.



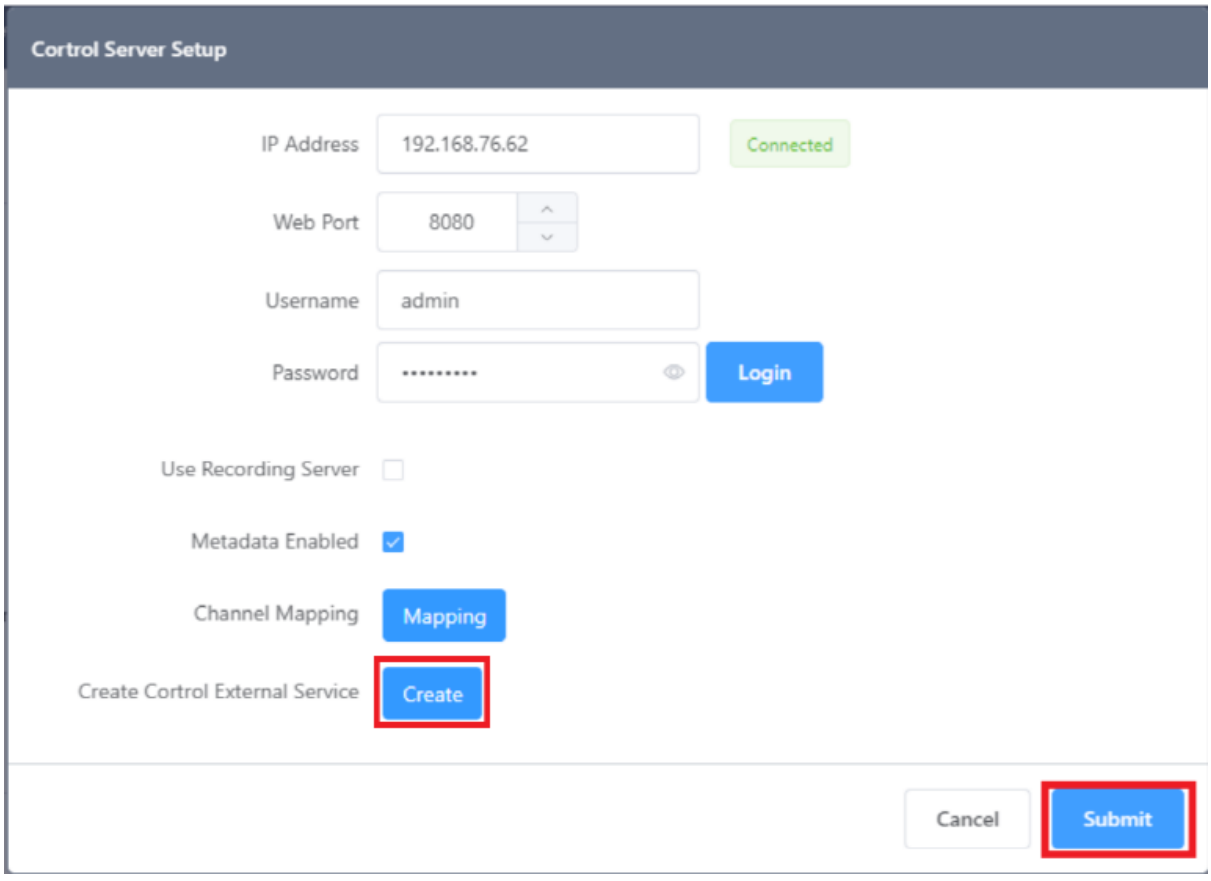

Channel test 1*
Channel
Details
Members
Membership
Permissions
Motion detector
Video analytics
Audio
Inputs 1
Outputs*
Channel configuration
Video overlays
Dewarp
Details
Title
test 1
Channel title
Main stream recording configuration
none
Change...
Recording configurtion assigned to the main video stream (includes supplementary streams by default)
Main stream storage
Default
Change...
Target storage for the main stream recording
Substream recording configuration
none
Change...
Recording configurtion assigned to the secondary video stream
Substream storage
Default
Change...
Target storage for the substream recording
Record supplementary streams with substream
Audio stream
VCA stream
Motion stream
Data stream
If enabled, the selected data stream will be recorded with the substream instead of the main stream
Video lost time
15
Video timeout interval in seconds, after which the video loss event is triggered
Passive mode
If enabled, server-device communication and video streaming will be paused until at least one client requests video
Recording identifier
FF6F33CD-37C1-441A-A53C-3489A2C819C2
Unique recording identifier of the current channel
Related items
Apply
OK
Cancel



Enter the **Recording identifier (UUID)** and press the **"Cameras update"** button to check if it is entered correctly. If the channel is connected successfully, green Connected is displayed.

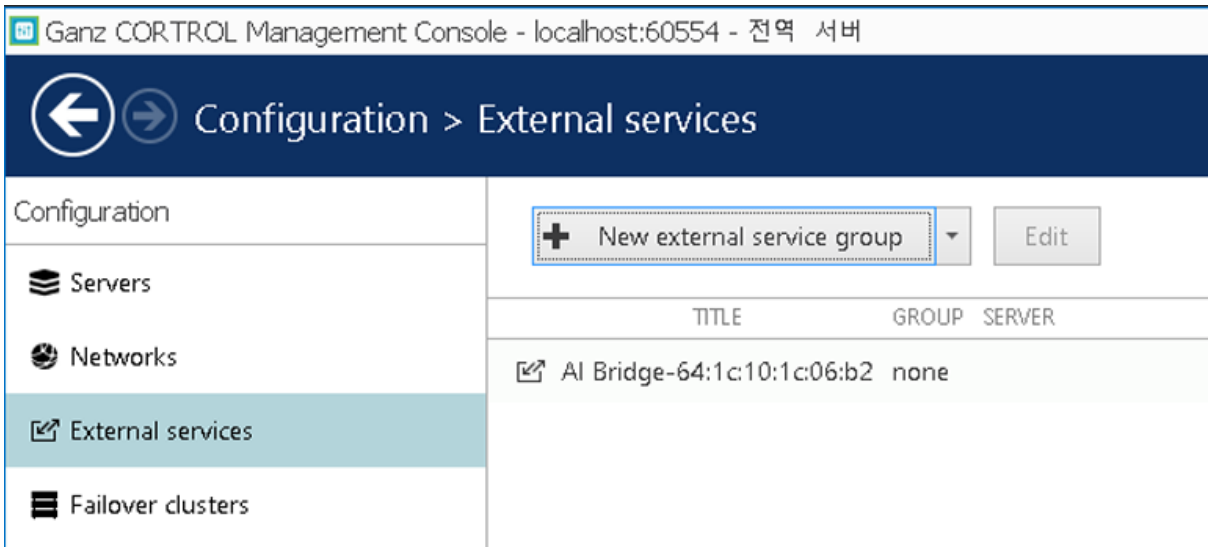
2.3 Create Evo External Service

Create an external service by clicking the **"Create"** button on AIBOX's "Evo VMS Setup page".

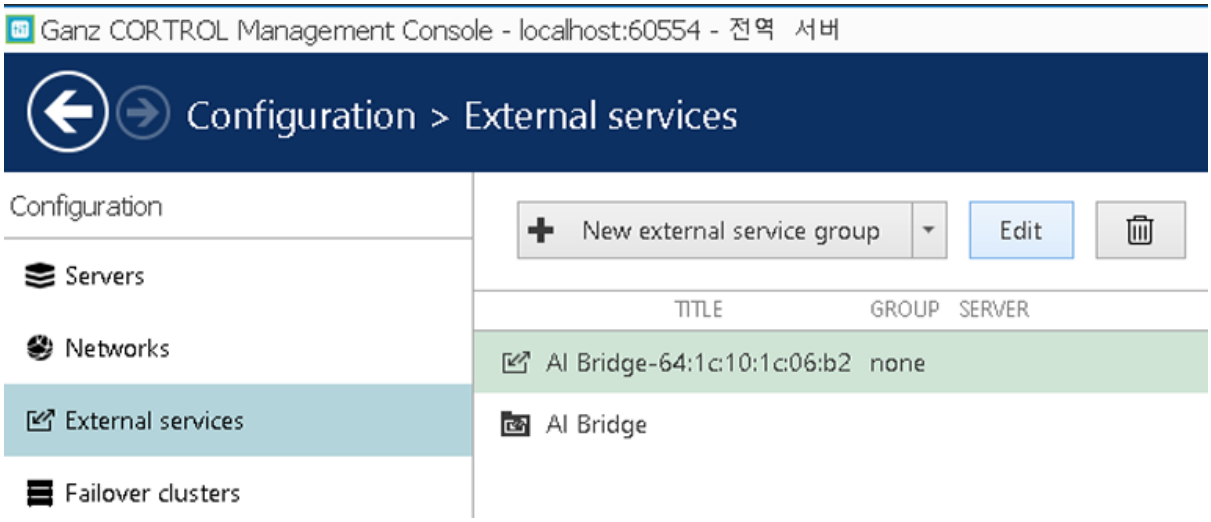


Note. Clicking Create will reset the Group mapping, so you will need to map it again. Rule settings and other configurations will not be reset.

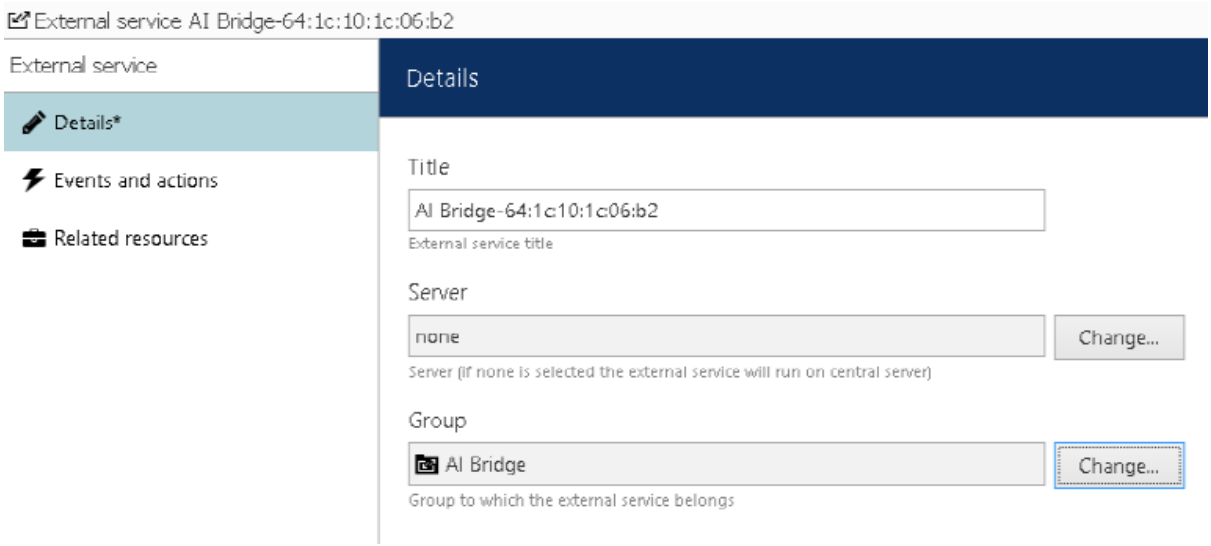
Next, Create an External Service Group.



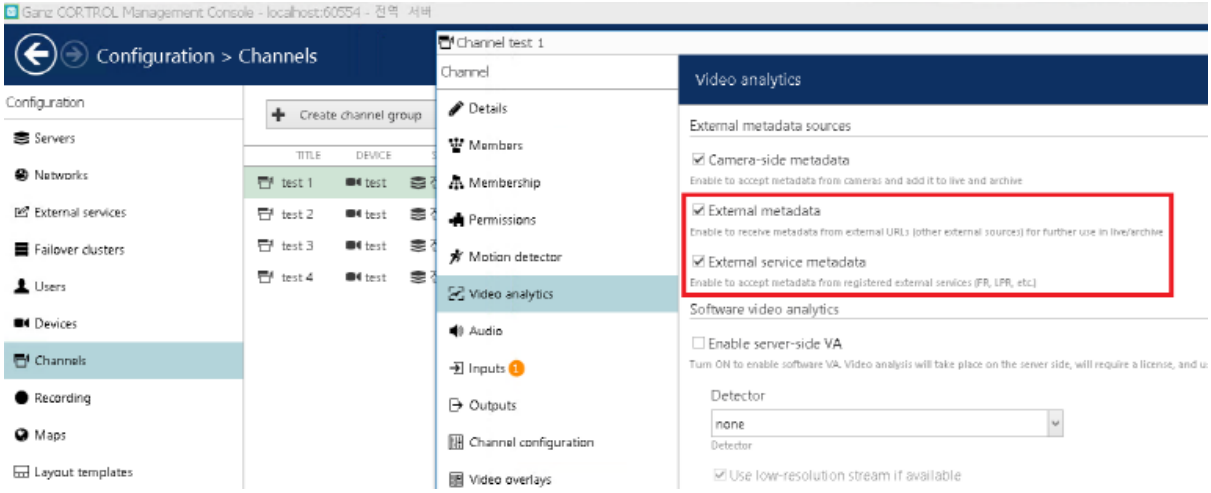
Enter the name of the new External Service Group as **“AIBOX”**.



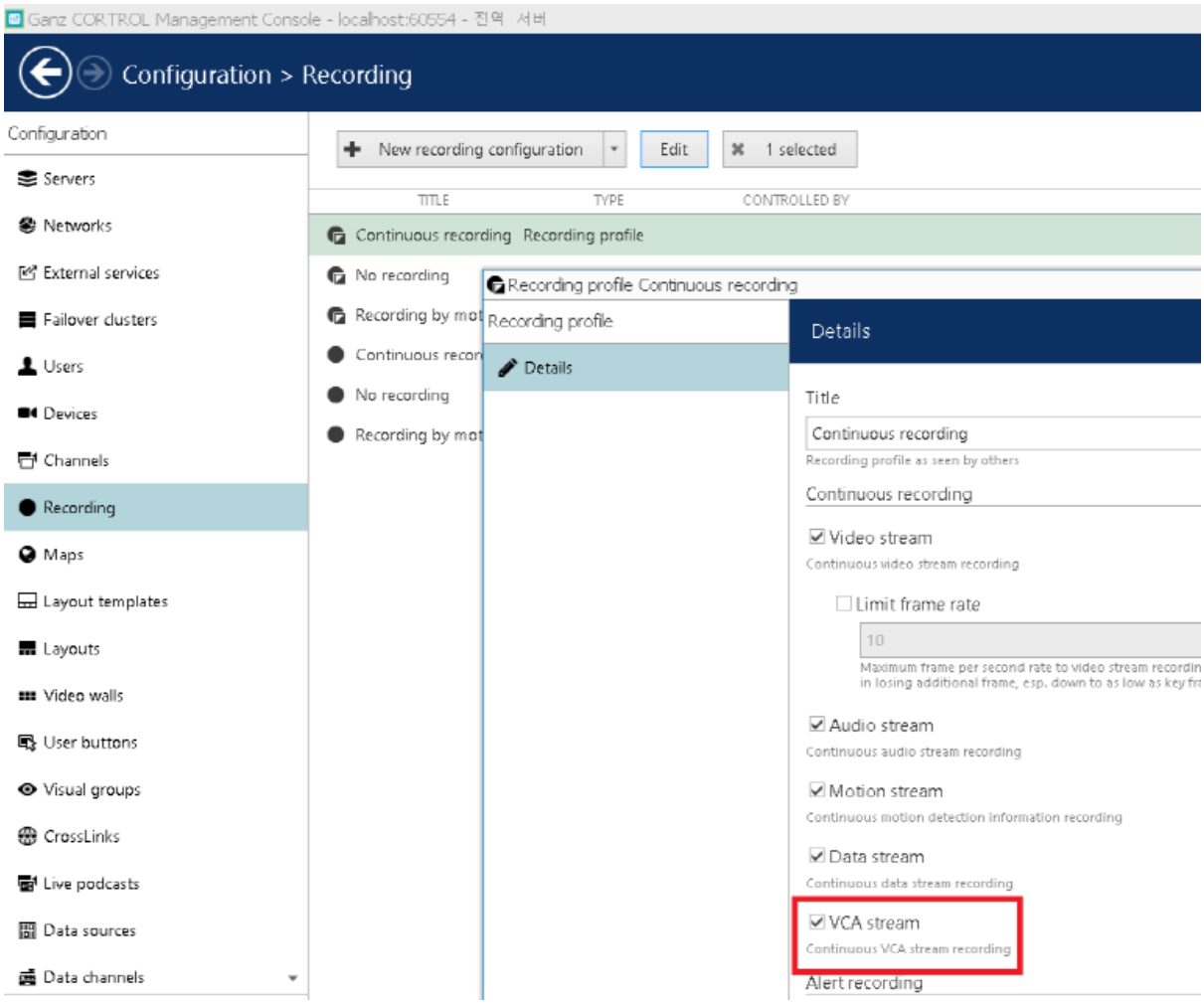
Assign AIBOX to the new External Service Group.



Note. If you are using the Evo Recording Server, please select the Evo Recording Server in the Server settings.



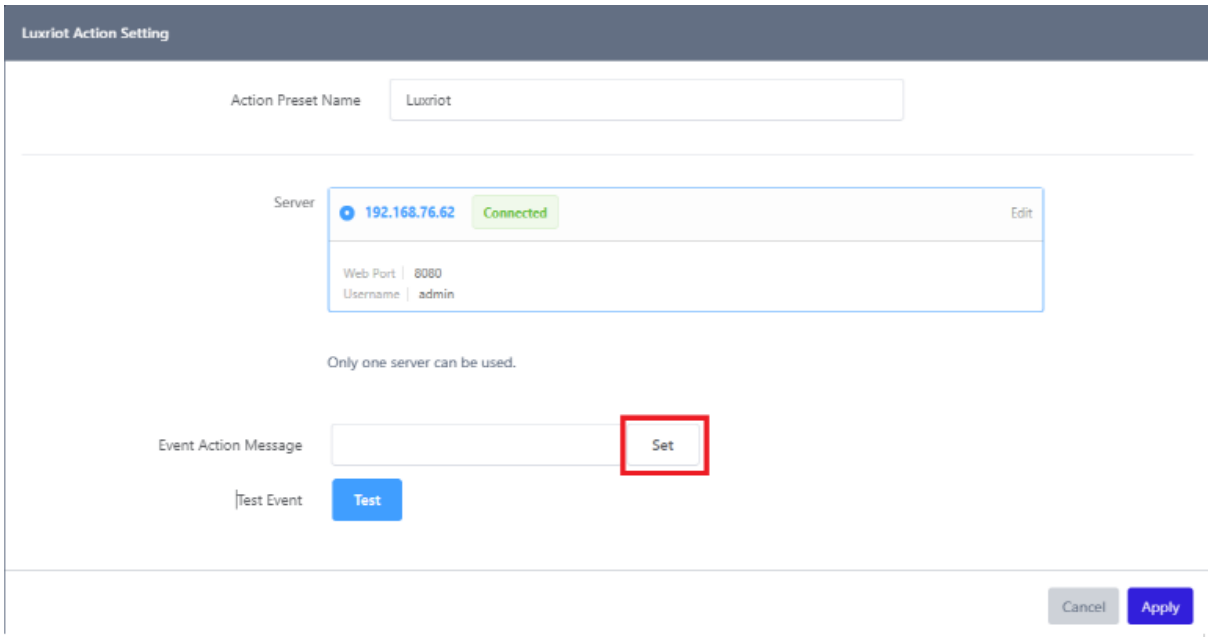
Note. To use the external service, you need to enable the external usage settings in every channel configuration. You need to configure this setting separately for each channel.



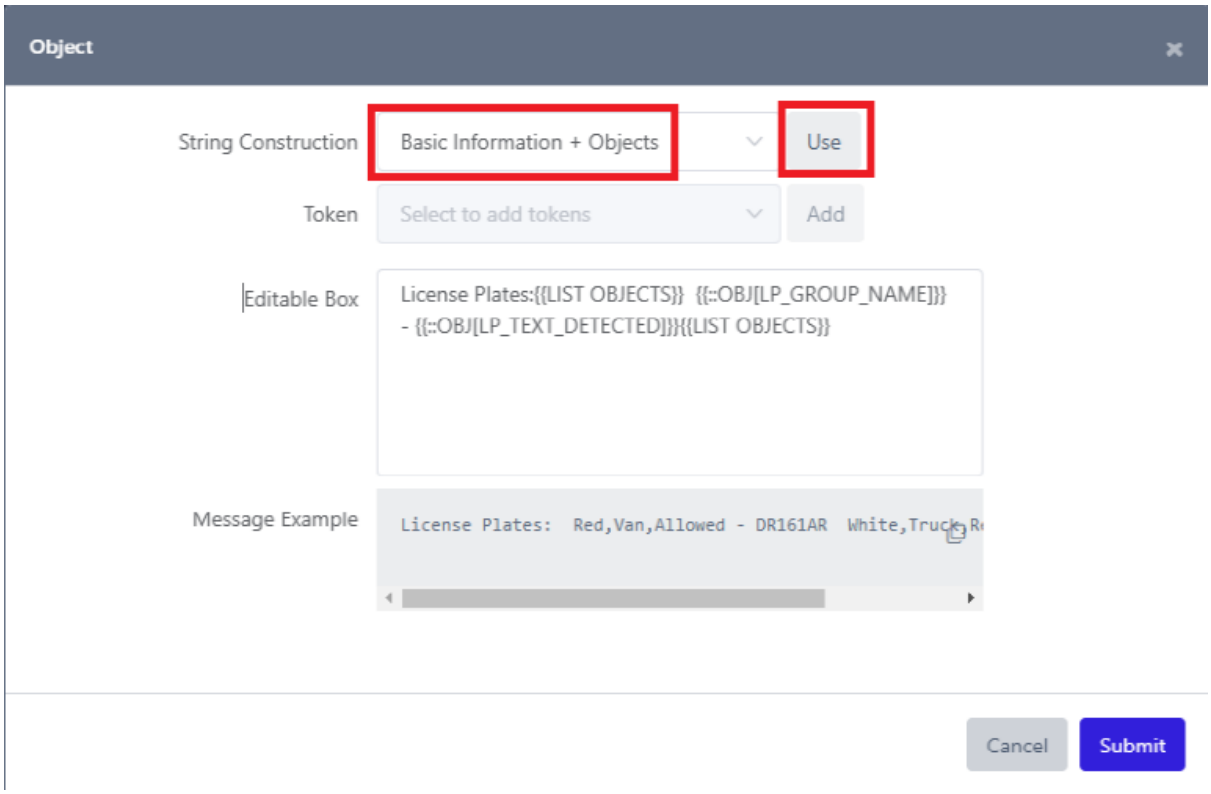
2.4 Set Event Action Message

With the Event Action message, you can configure the message format that is sent to Luxriot when an event occurs in AIBOX. For example, you can add LPR information or counting data to the message, which can then be viewed in Luxriot.

Click the “Set” button to configure the Event Action Message.

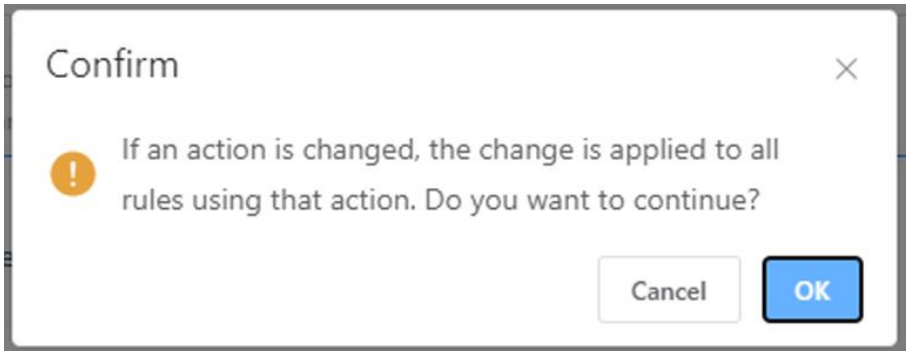


Select the desired event message, then click ‘Use’ to configure the event action message.



Note. In Evo version 1.27.0.1366, there are multilingual issues and line breaks are not recognized properly, so data must be sent in a single line.

Click the **“Apply”** button to save the Evo Server settings.

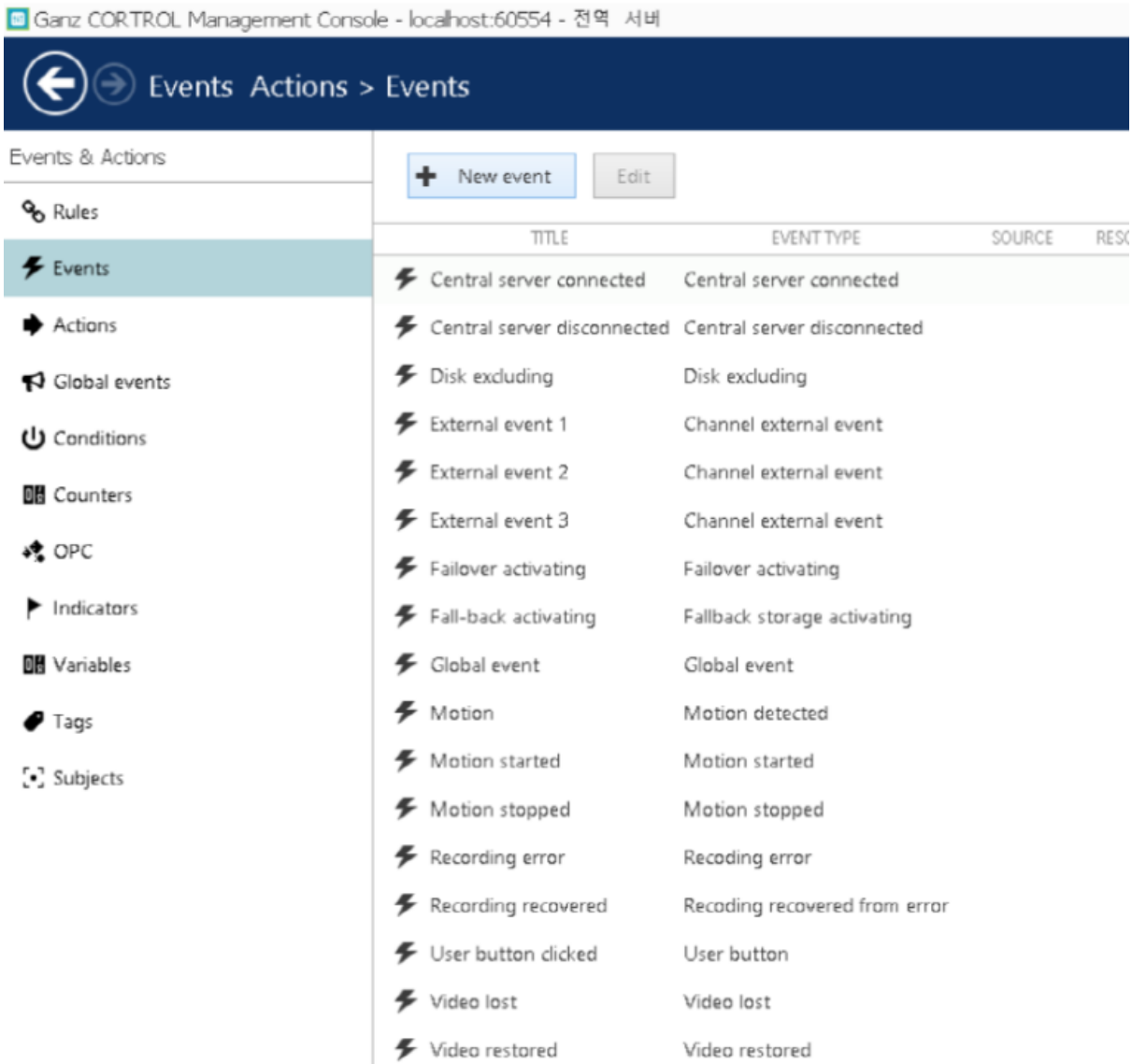


If you see the device registered in the format **"AIBOX-MacAddress"** in the External Service tab of the Evo Management Console, it's OK.

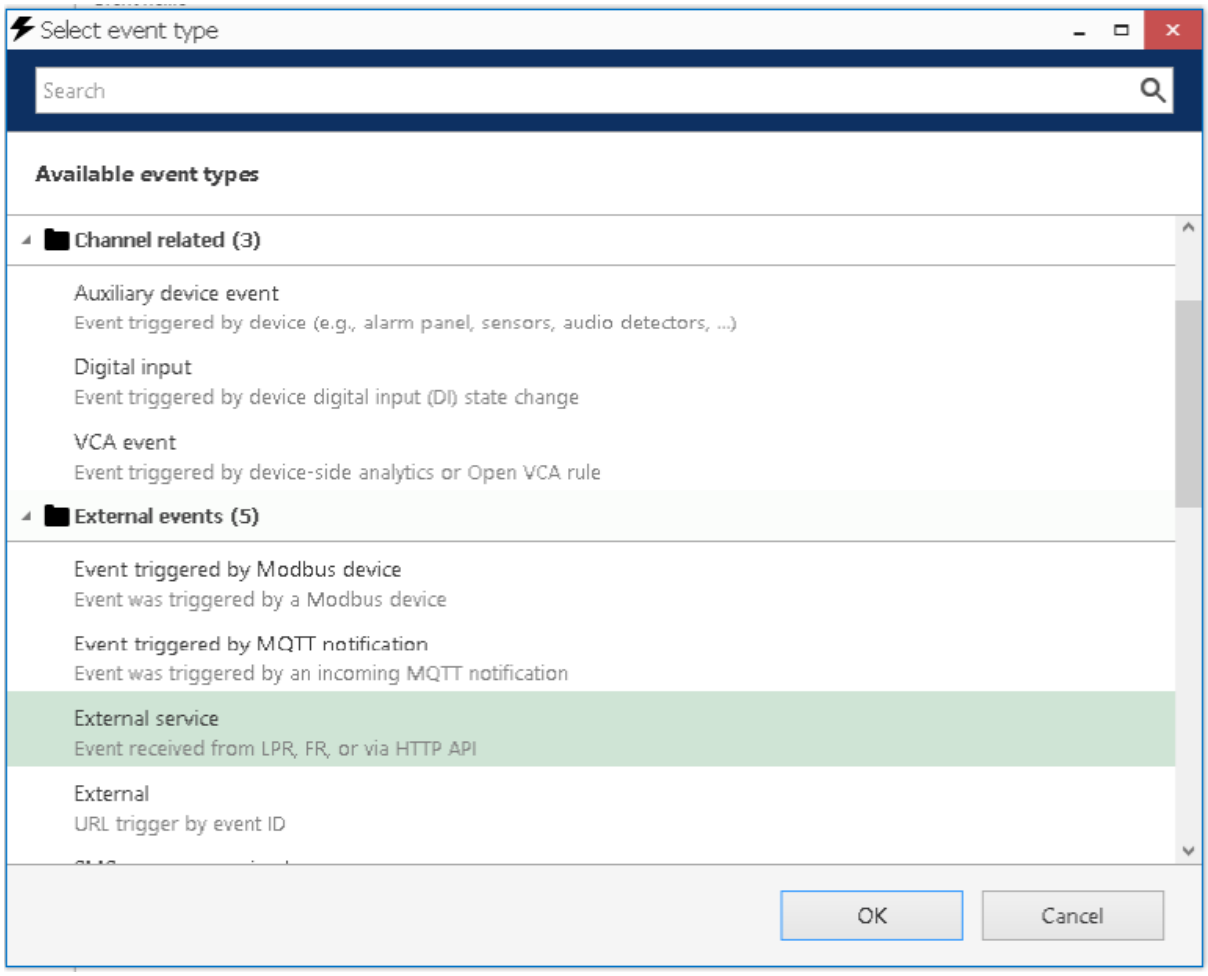
2.5 Create Evo Event & Rule

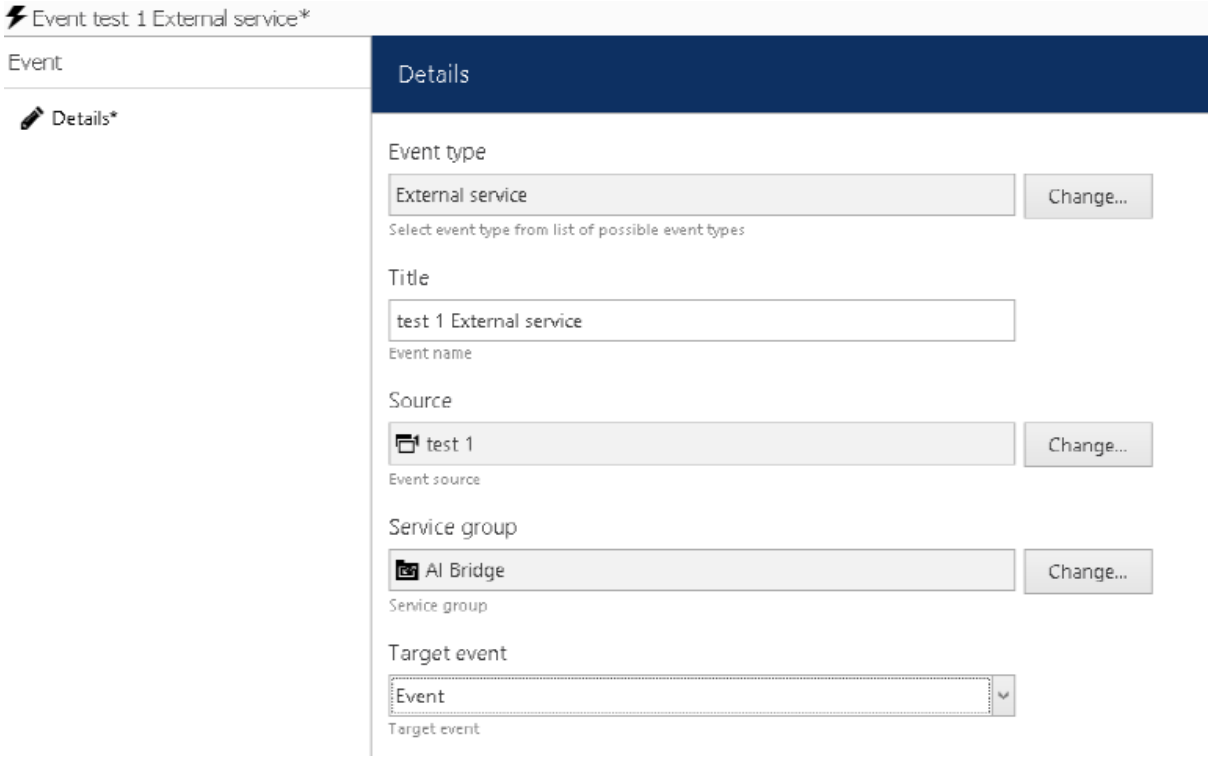
We need to configure the events, actions, and rules that will be sending notifications

Click the **"New Event"** button to add a new event.

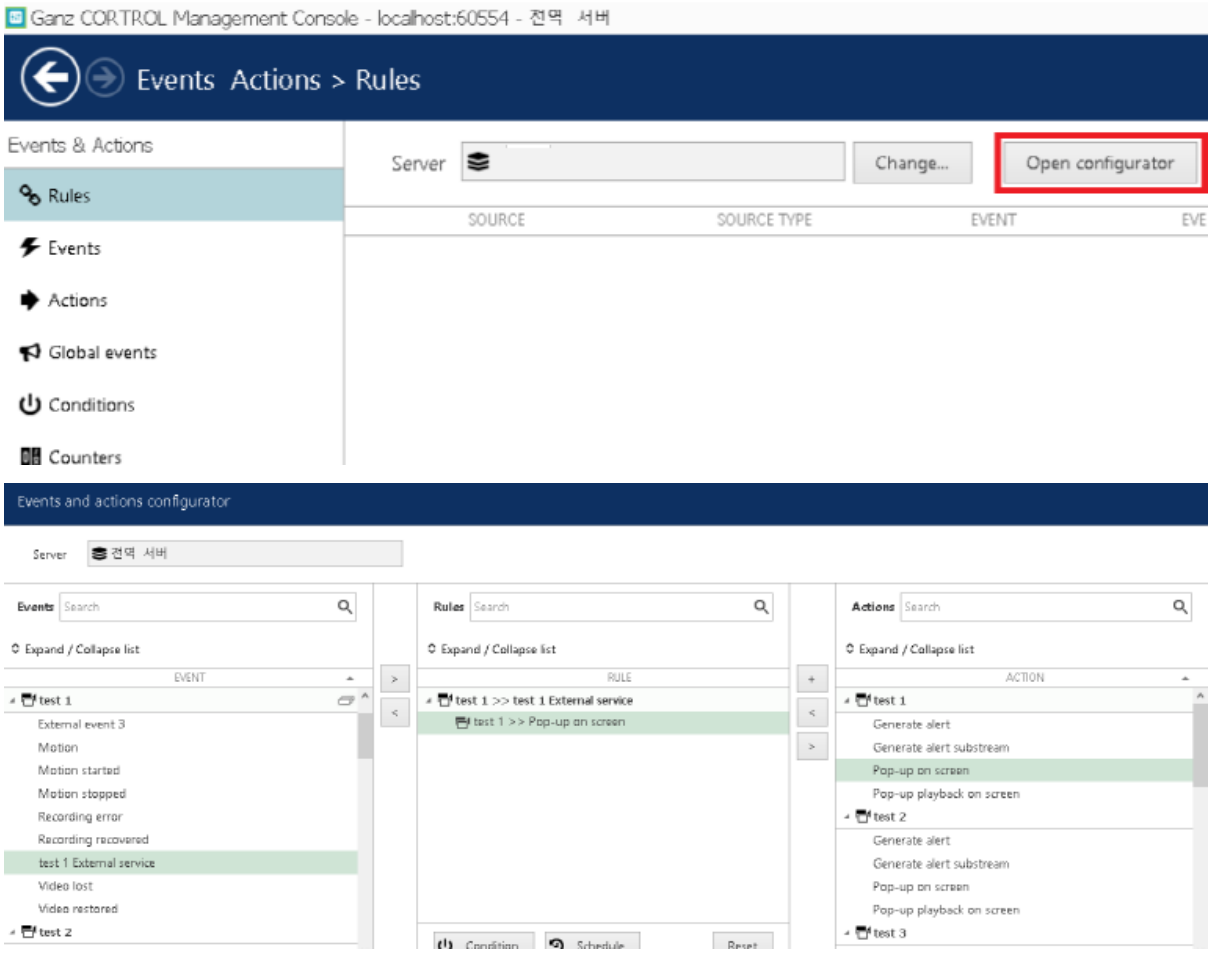


Select Event Type as **External Event – External Service.**





Create a rule by combining the created event type and action.



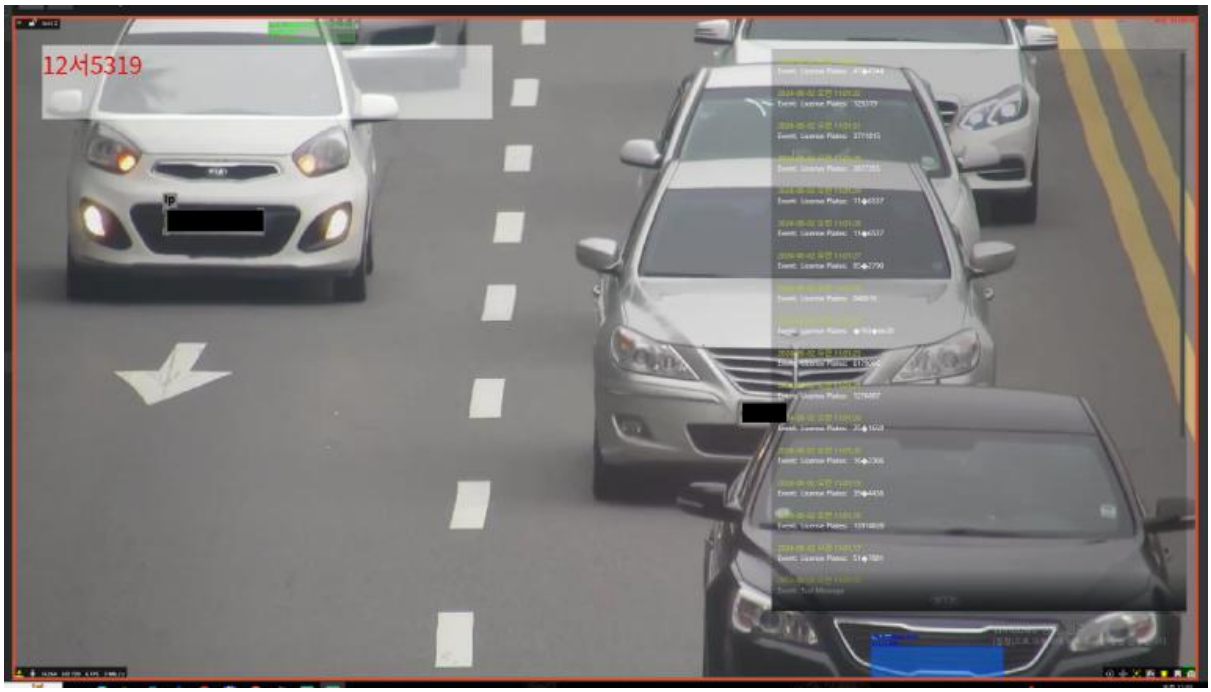
3. Demo

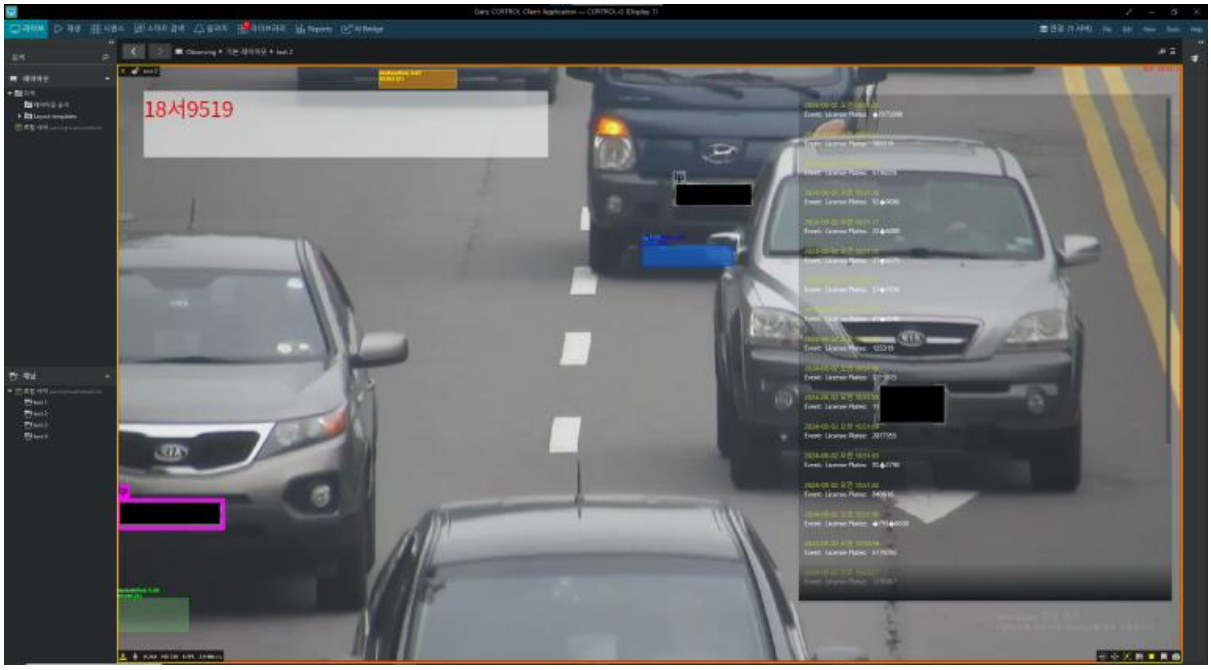
3.1 Live

Set the Evo Client to display metadata and alarms to check if it works with AIBOX.

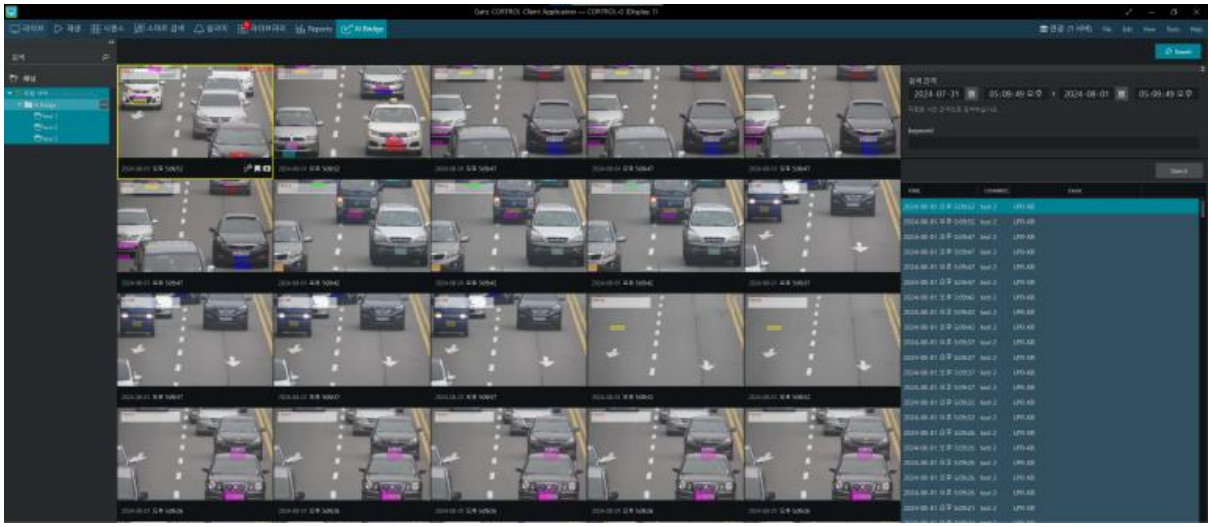
Click the icon at the bottom of the video.


12서5319


12서5319



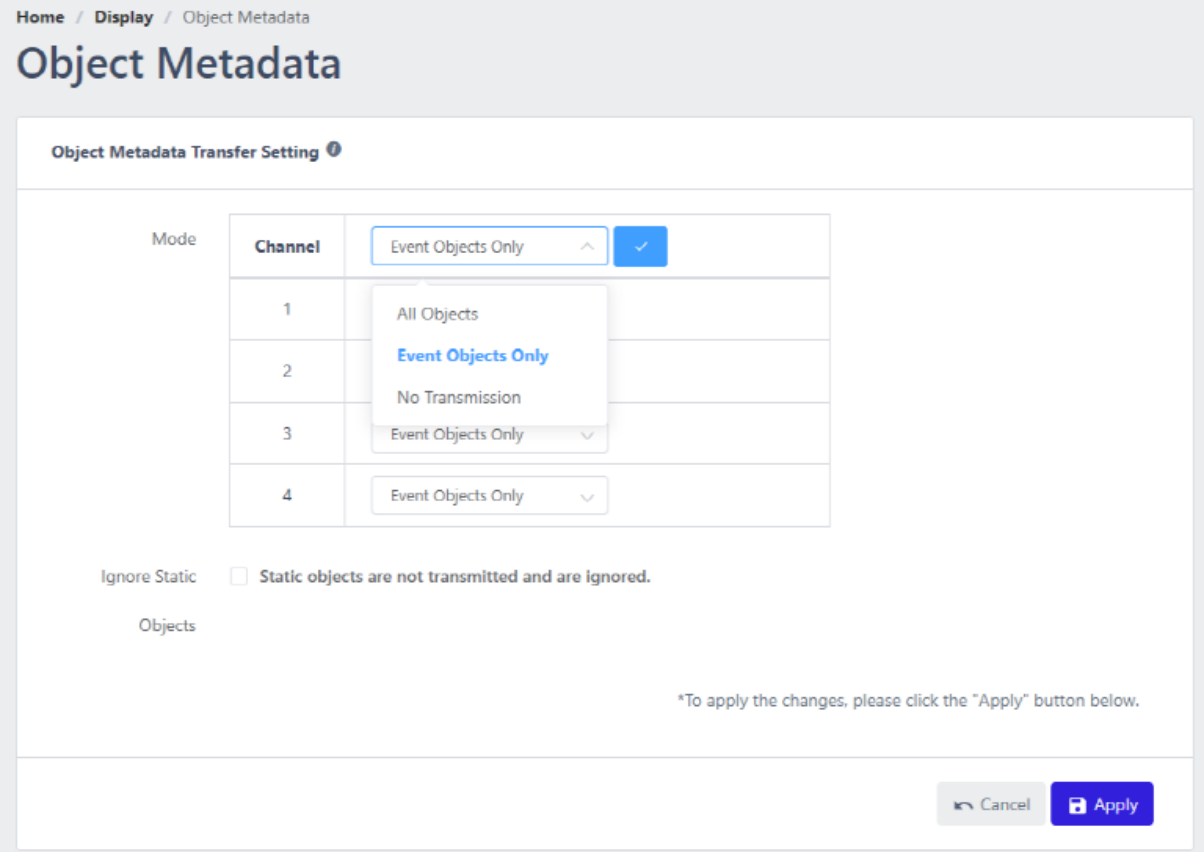
3.2 Search



4. FAQ

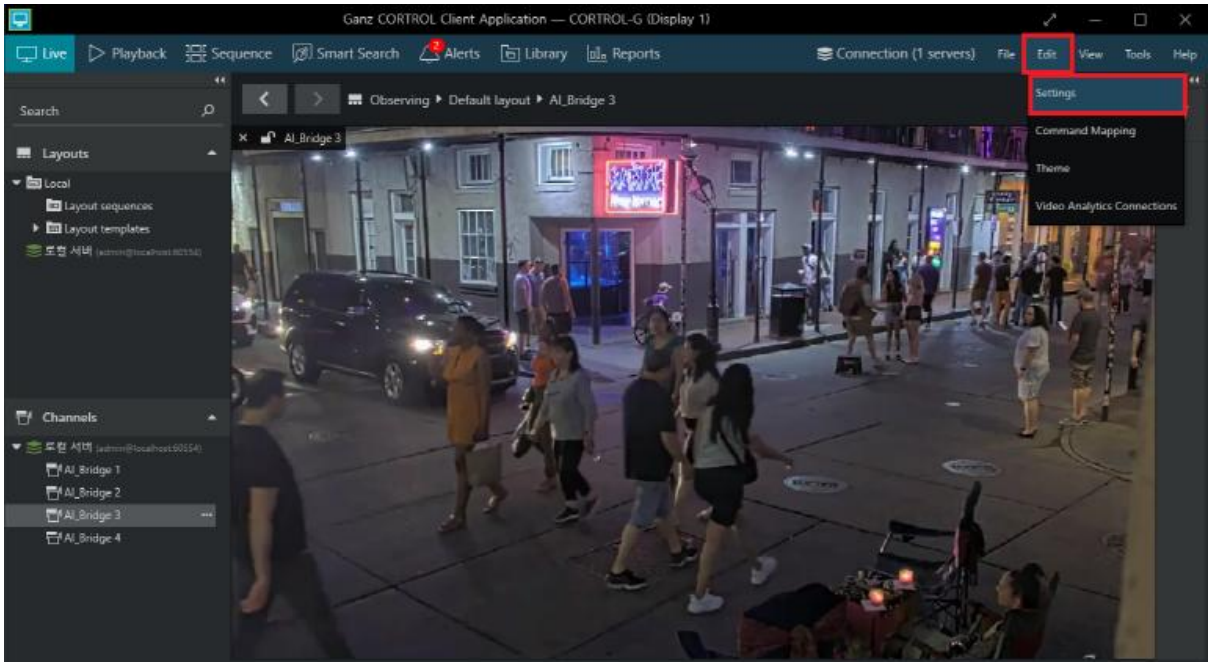
4.1 Object Metadata Transfer Options

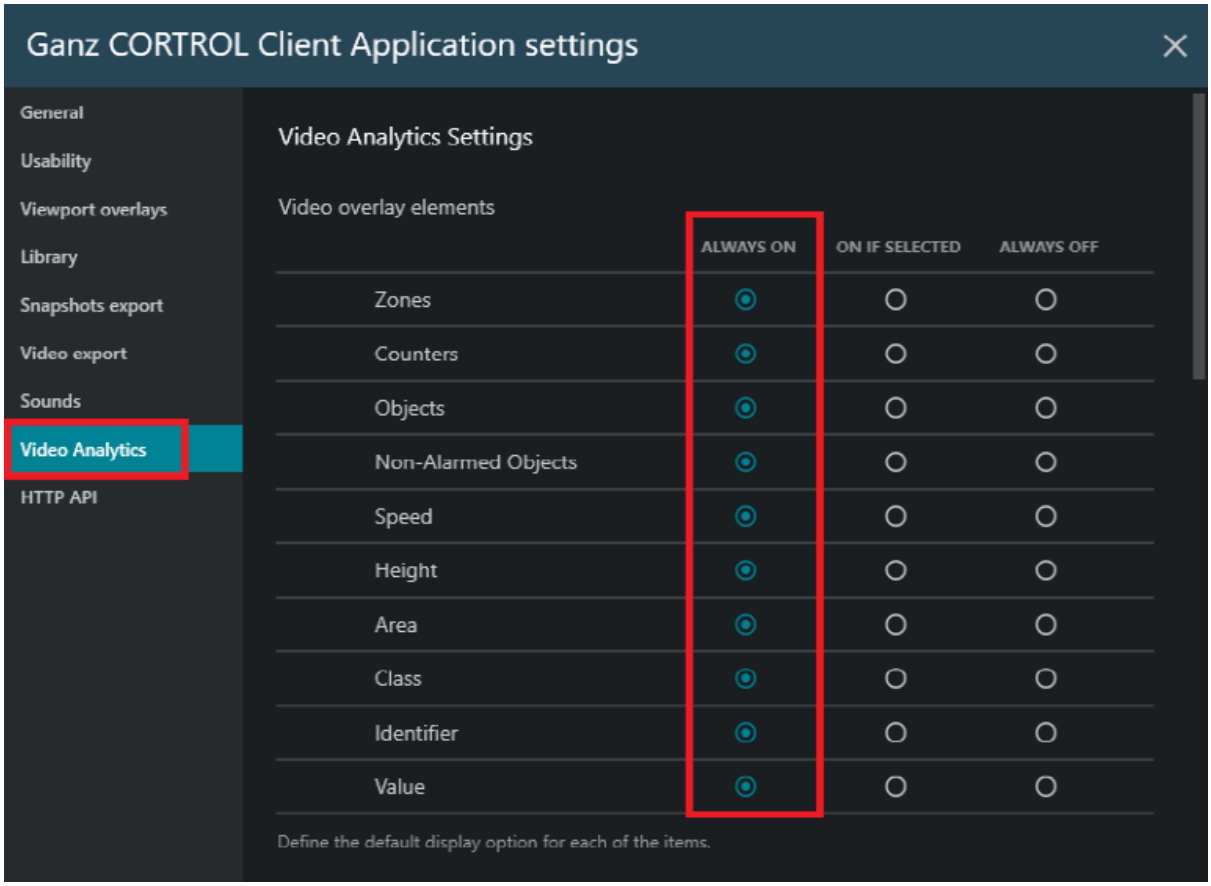
If this feature is turned OFF, ONVIF Metadata and the Metadata set in the Plugin will not be transmitted. This applies to the overall operation of Metadata.



4.2 Evo Client Side Video Analytics Overlay Settings

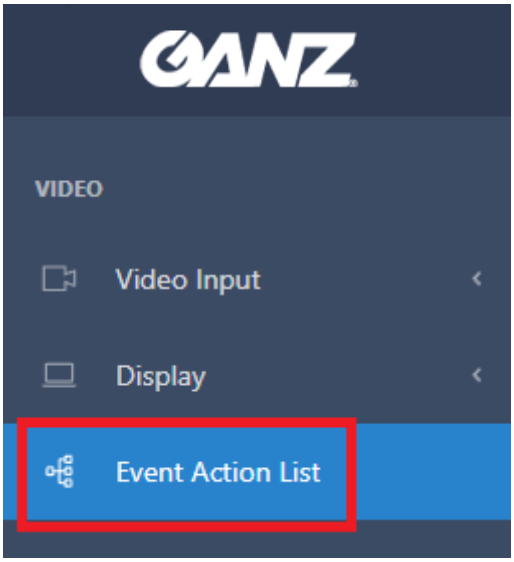
If Video Analytics is not enabled in the Settings under Edit in the Evo Client Application, metadata may not function correctly. The default value is ON, so do not turn this feature off.



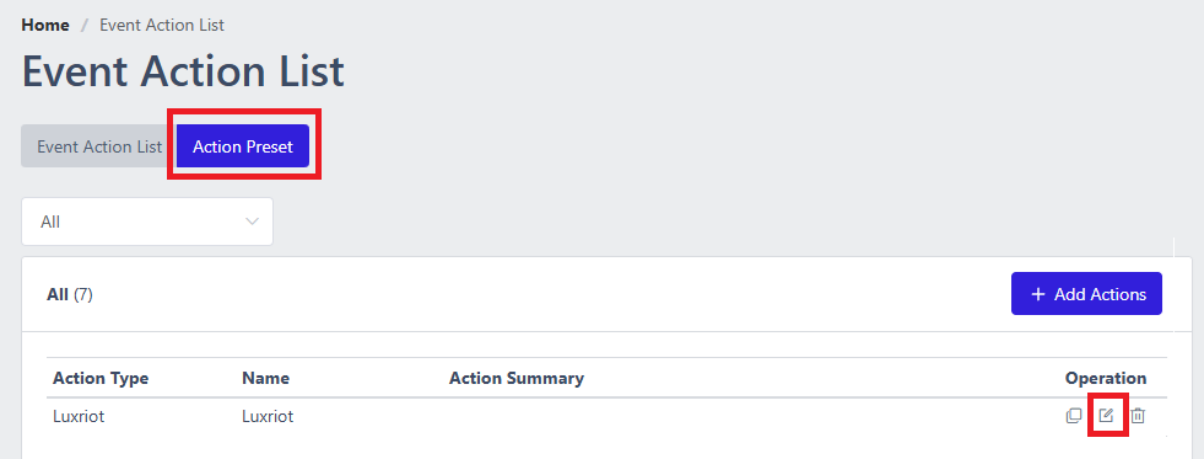


4.3 Check the connection between AIBOX and Luxriot Evo

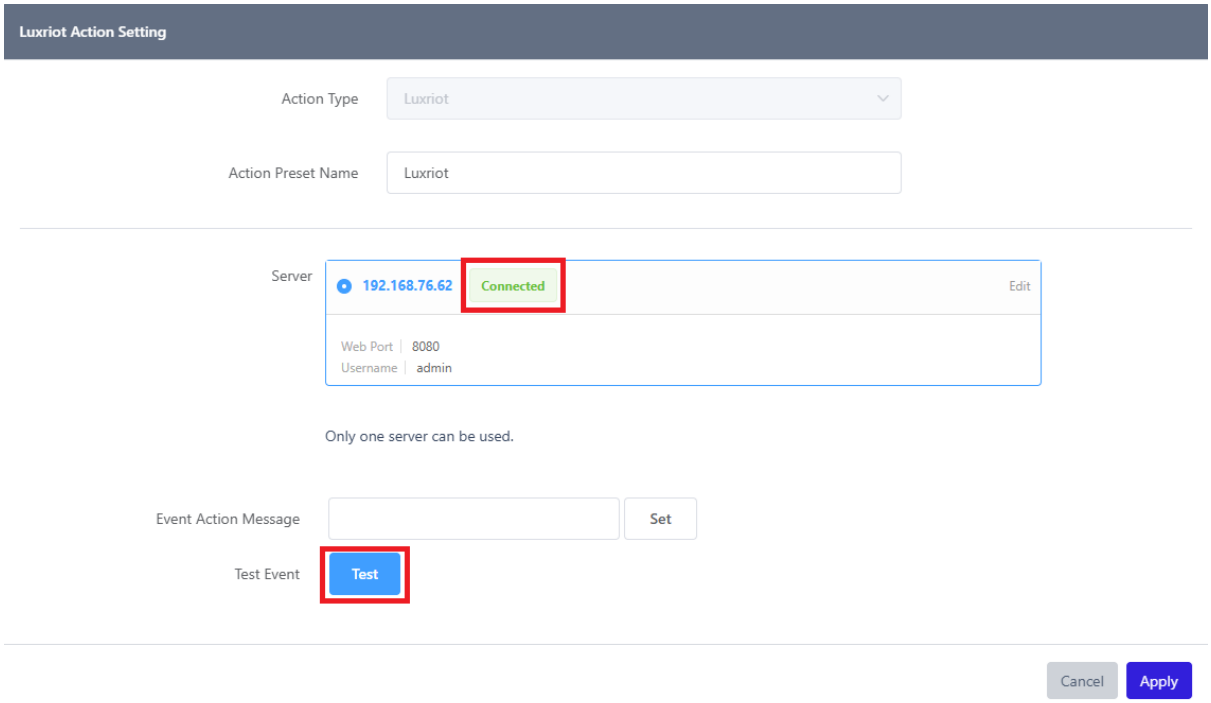
Click on “Event Action List” under “VIDEO” in the AIBOX webpage.



Enter “Action Preset” and click the Luxriot settings button that was configured earlier.

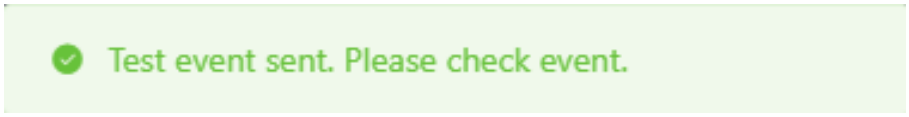


If it is confirmed that you are connected to the Luxriot Server, click the “Test” button.

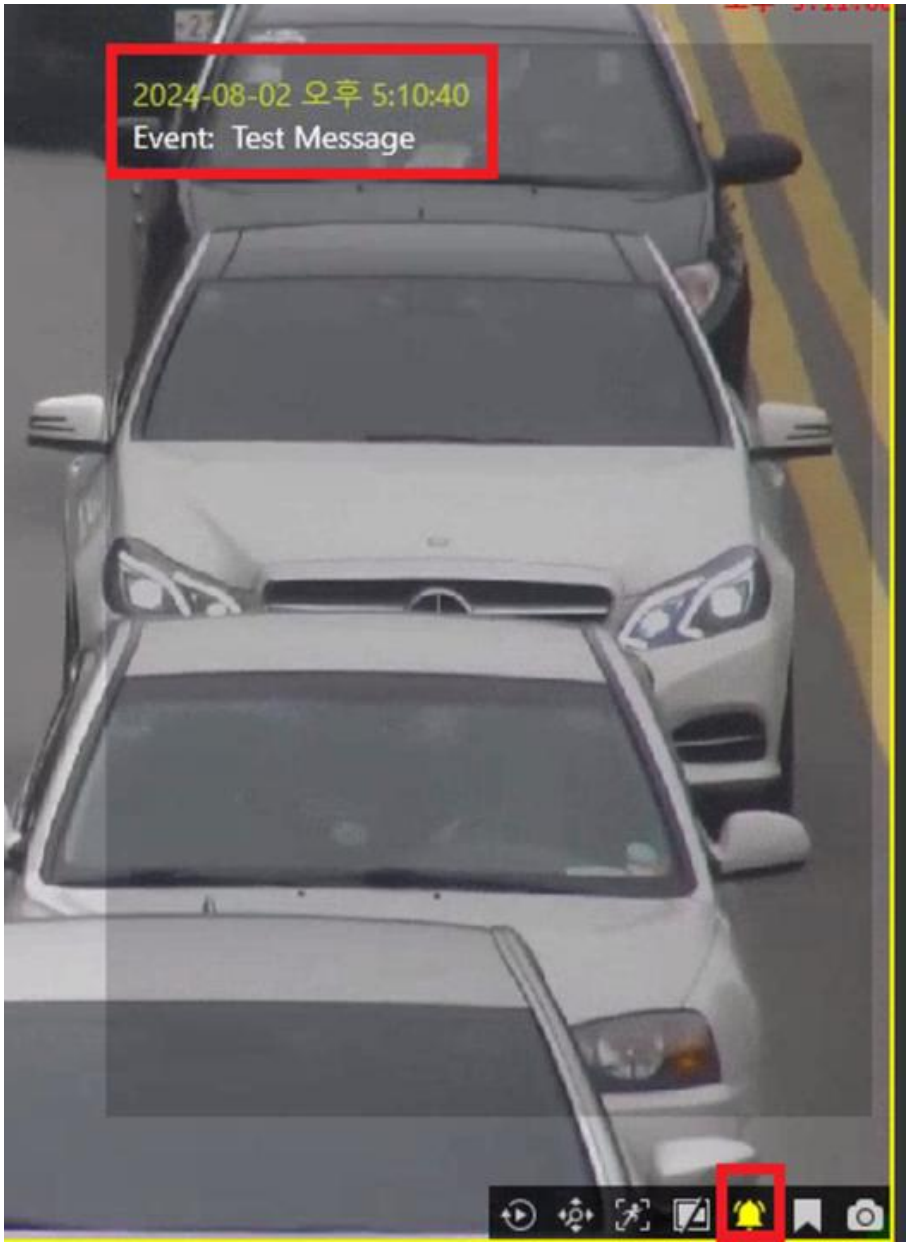


Note. Before clicking the TEST button, ensure that the green Connected button is visible on the Evo Server. If the gray Disconnected indicator is displayed, please check the server settings.

After clicking the “Test” button, if the message is successfully sent, a pop-up like the one below will appear.



Now, go to Luxriot Evo and check the alarm message.



Milestone XProtect Integration Guide

1. Introduction

1.1 Prerequisites

- AIBOX FW version 102700 or greater.
- Milestone XProtect 2023 R1 or greater.

1.2 Learn about integration architecture

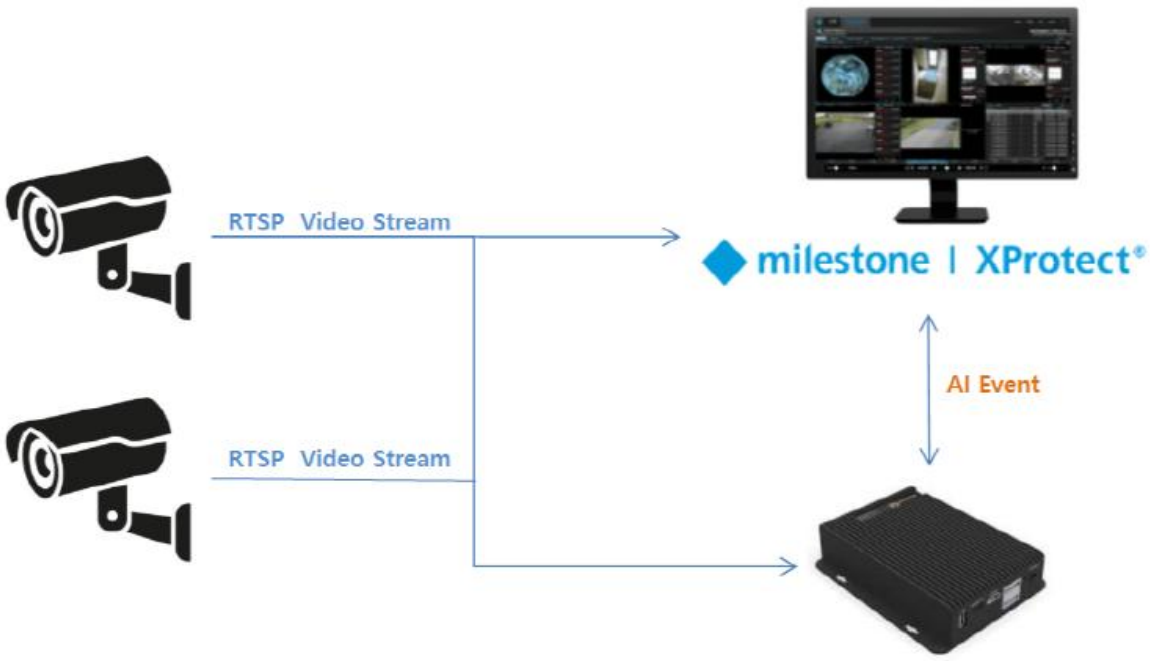
There are two ways to integrate AIBOX with Milestone XProtect VMS:

1) Case 1

The AIBOX receives the RTSP video stream from the IPCAM and provides the annotated video and event data after AI analysis. The annotated video is transcoded to provide object recognition information, bounding boxes, zone information, and more from AIBOX's AI analysis.

2) Case 2

Both AIBOX and Milestone XProtect VMS simultaneously receive the RTSP video stream from the IPCAM, and the AIBOX sends the AI analysis events to XProtect VMS. It can also receive the RTSP stream from Milestone XProtect VMS instead of the IPCAM's RTSP video stream.



2. Configuration

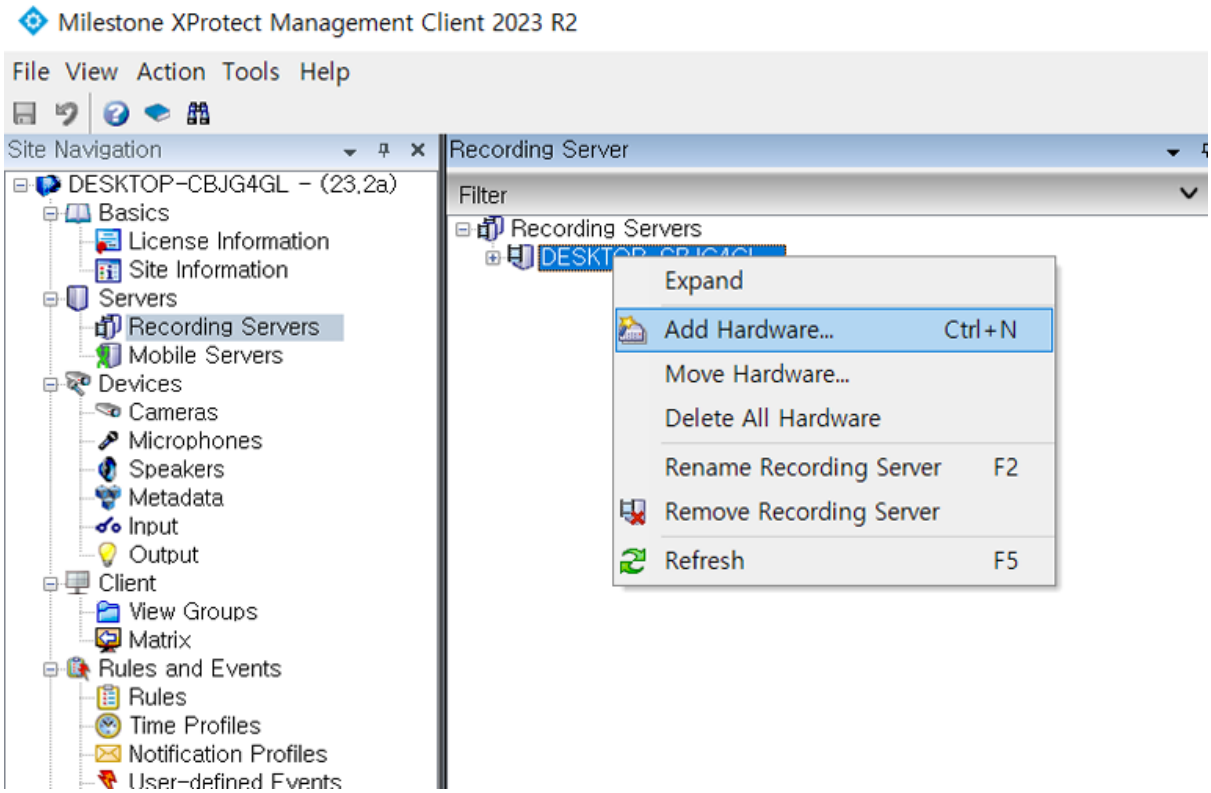
2.1 Milestone xProtect VMS Configuration

We will explain how to integrate AIBOX with Milestone XProtect VMS using the Case1 method.

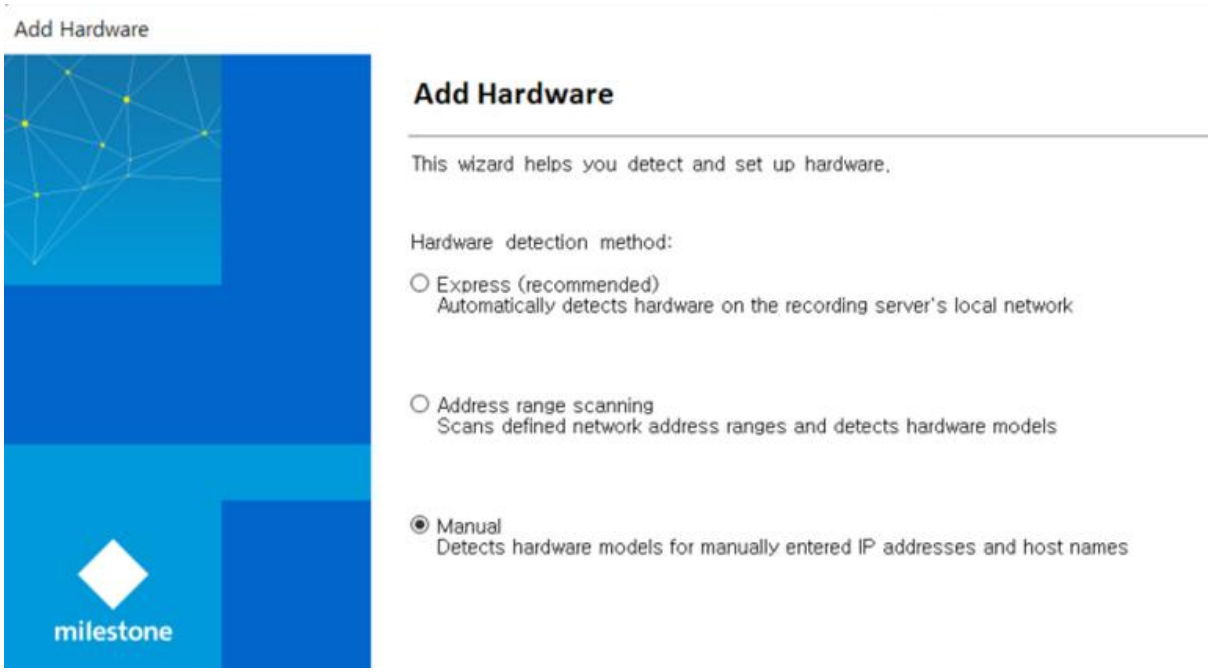
Note: For the Case2 integration type, you can skip step 1(Adding the AIBOX to Milestone XProtect VMS) and proceed from step 2(Enable the XProtect analytics events).

1) Adding the AIBOX to Milestone XProtect VMS.

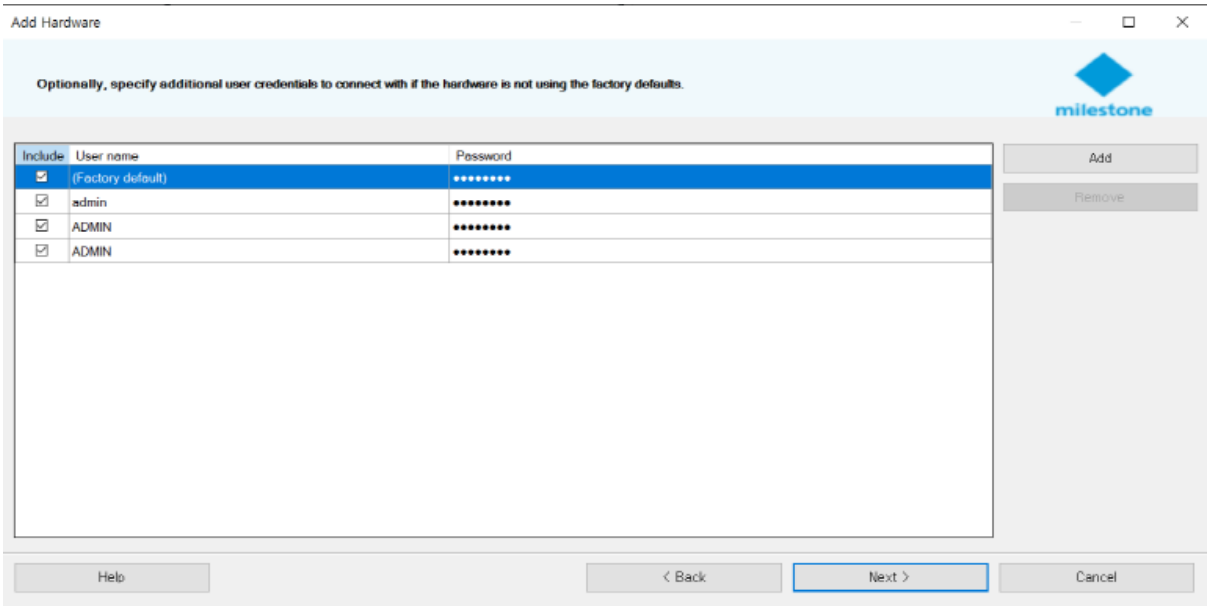
In the XProtect Management Client, select "**Add Hardware**".



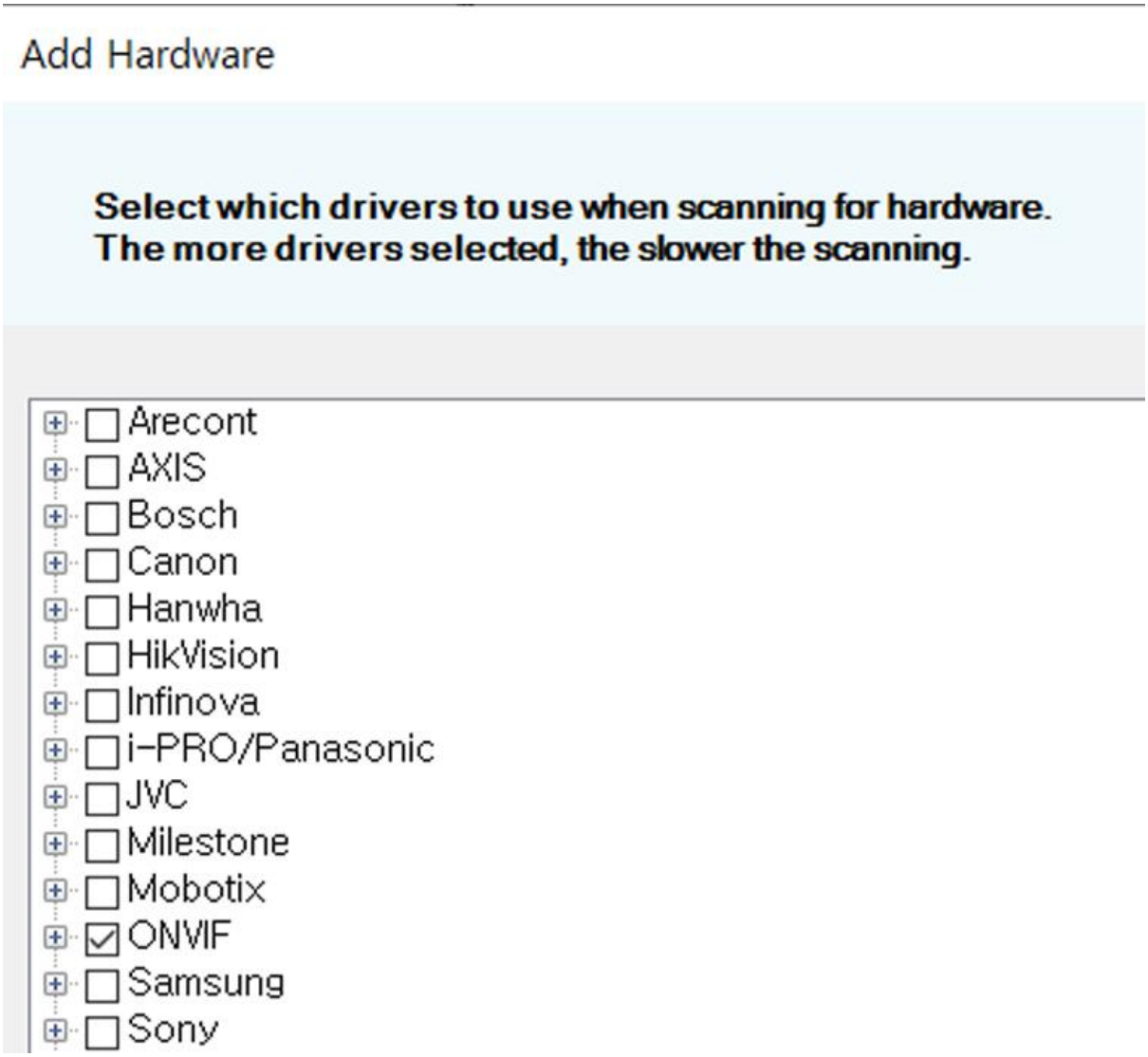
If you know the IP address of the AIBOX device, choose "**Manual**".



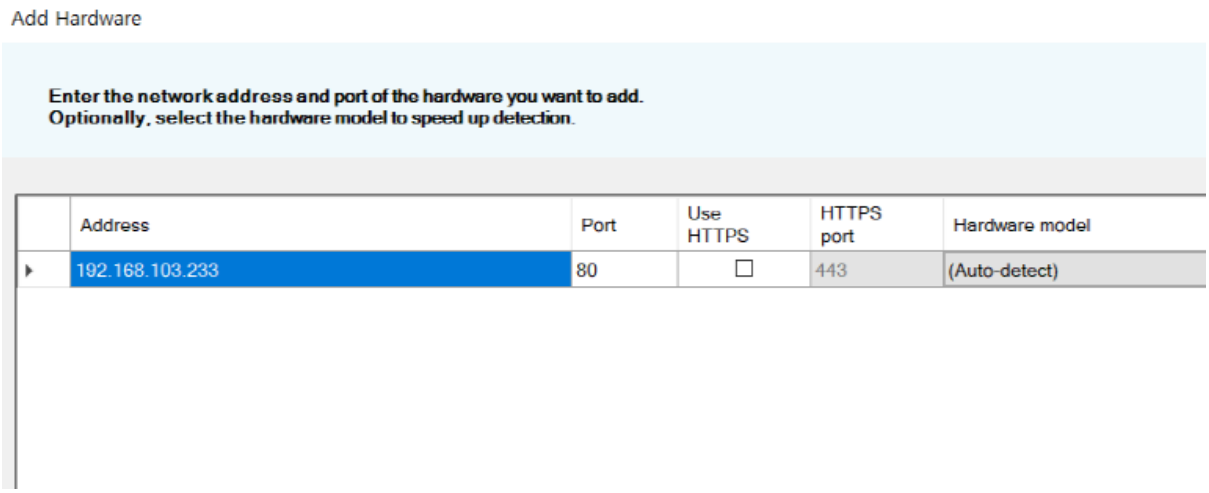
Enter the **login** information for the AIBOX.



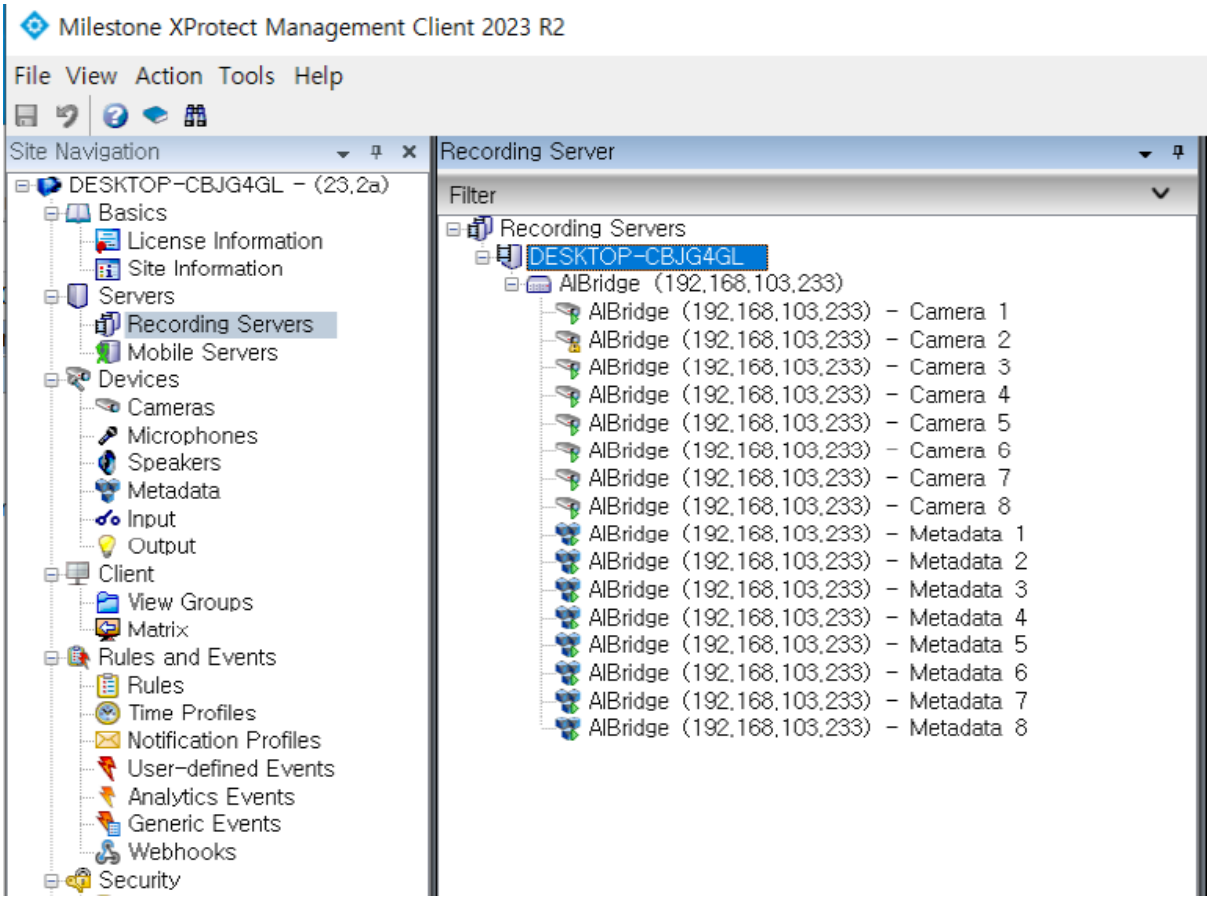
Select **“ONVIF”** from the device driver options.



Enter the IP address information of the AIBOX. If you haven't changed the onvif service port settings of AIBOX, the Port is 80. HTTPS is not used.

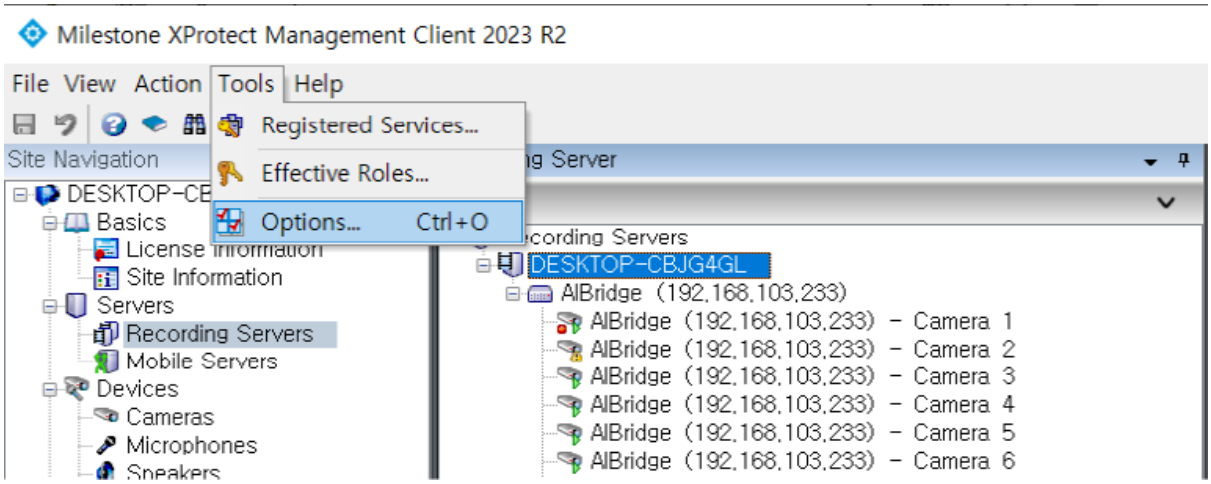


Add the detected AIBOX hardware and change the name as desired. If this fails, recheck the setup and try again.

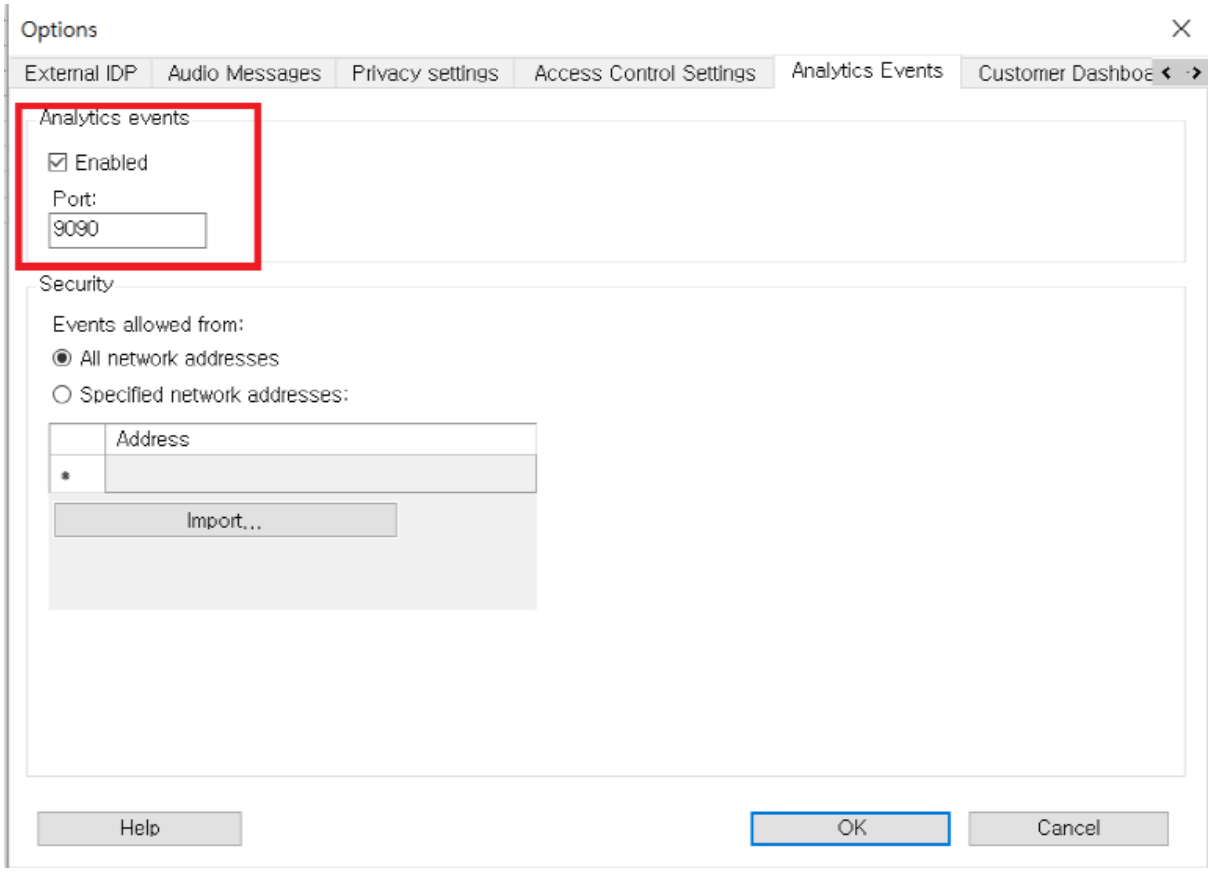


2) Enable the XProtect analytics events

Click on the **Tools > Options** menu in the XProtect Management Client.

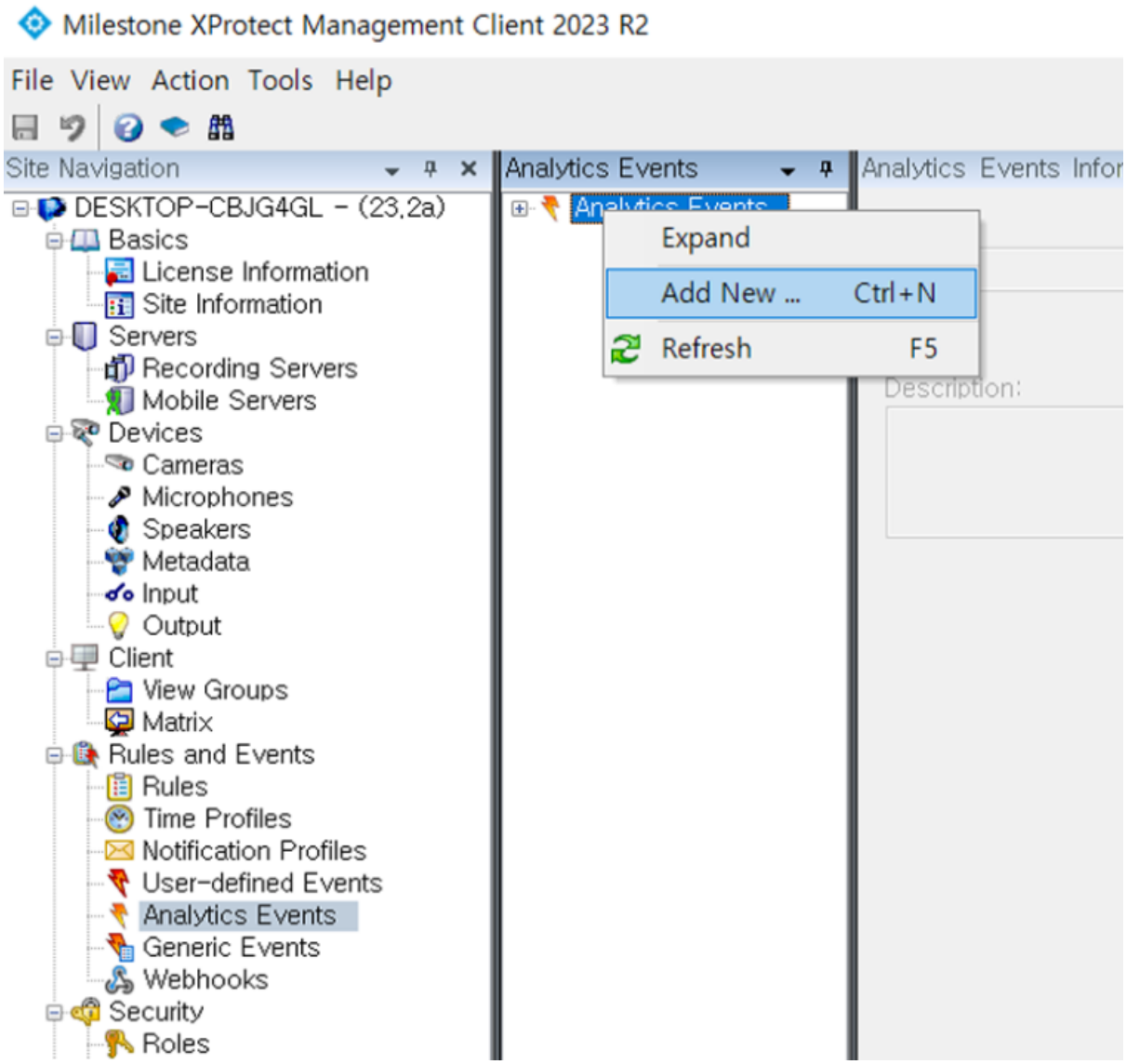


In the Analytics Event tab, check the **Enabled** checkbox. The service port must be open in the firewall. If you change the service port, you must enter the same port number when registering the AIBOX's Milestone action handler.

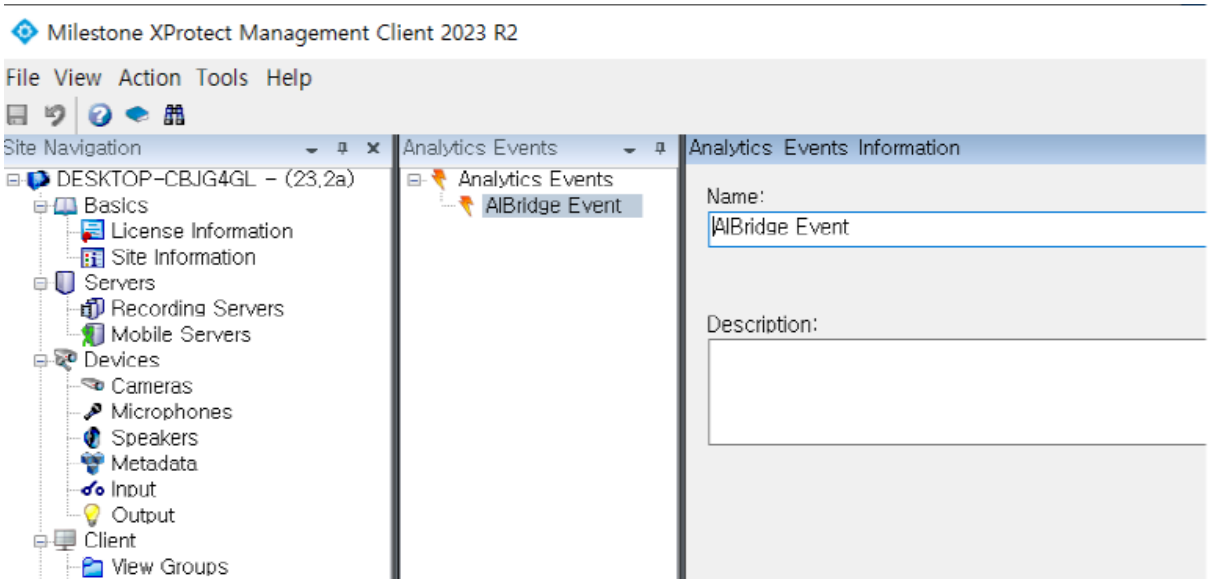


3) Add analytics events and alarm definitions.

In the XProtect Management Client, select "**Analytics events**" from the left panel, right-click, and choose "**Add New**".



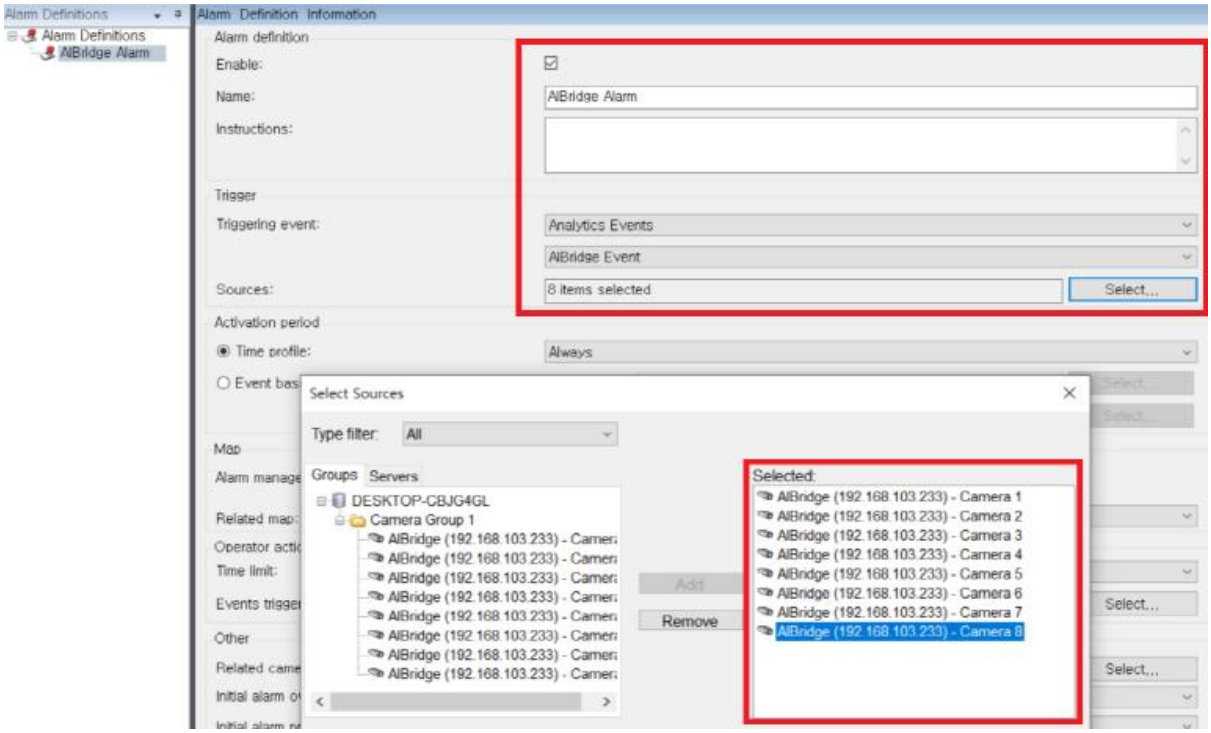
Enter the event name as "**AIBOX Event**". This value is an essential key for distinguishing events between AIBOX and XProtect. It must be entered in the "**Message key**" property in the Milestone Action handler settings of AIBOX.



In the XProtect Management Client, add "**Alarm definitions**".

Select "**Analytics Events**" for the Trigger Event item, and choose the "**AIBOX Event**" you added earlier. For the Trigger Source item, add the channel of the AIBOX.

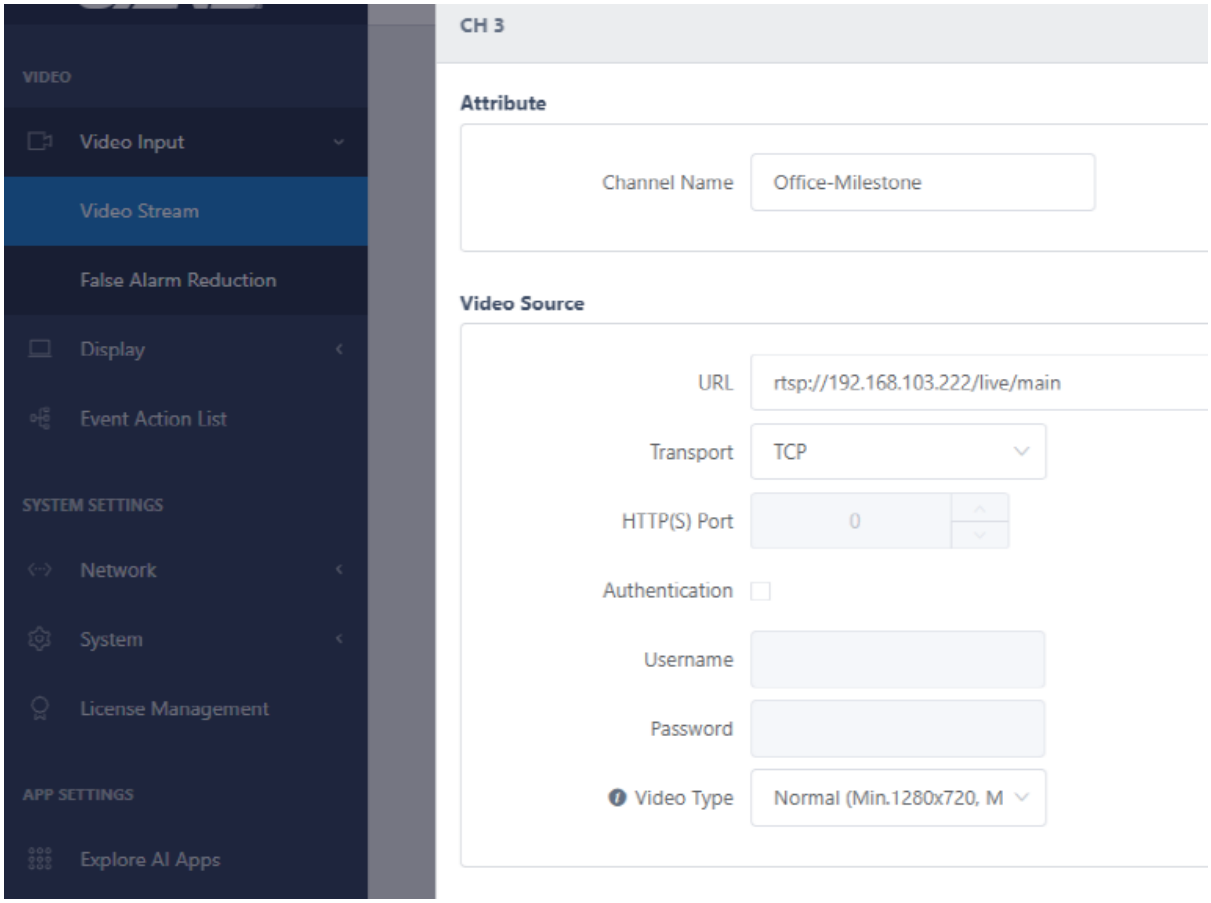
Note: When registering the Trigger Source, if you add the IPCAM channel instead of the AIBOX camera channel, it operates as the Case2 integration type.



2.2 AIBOX Configuration

1) Add Video Stream

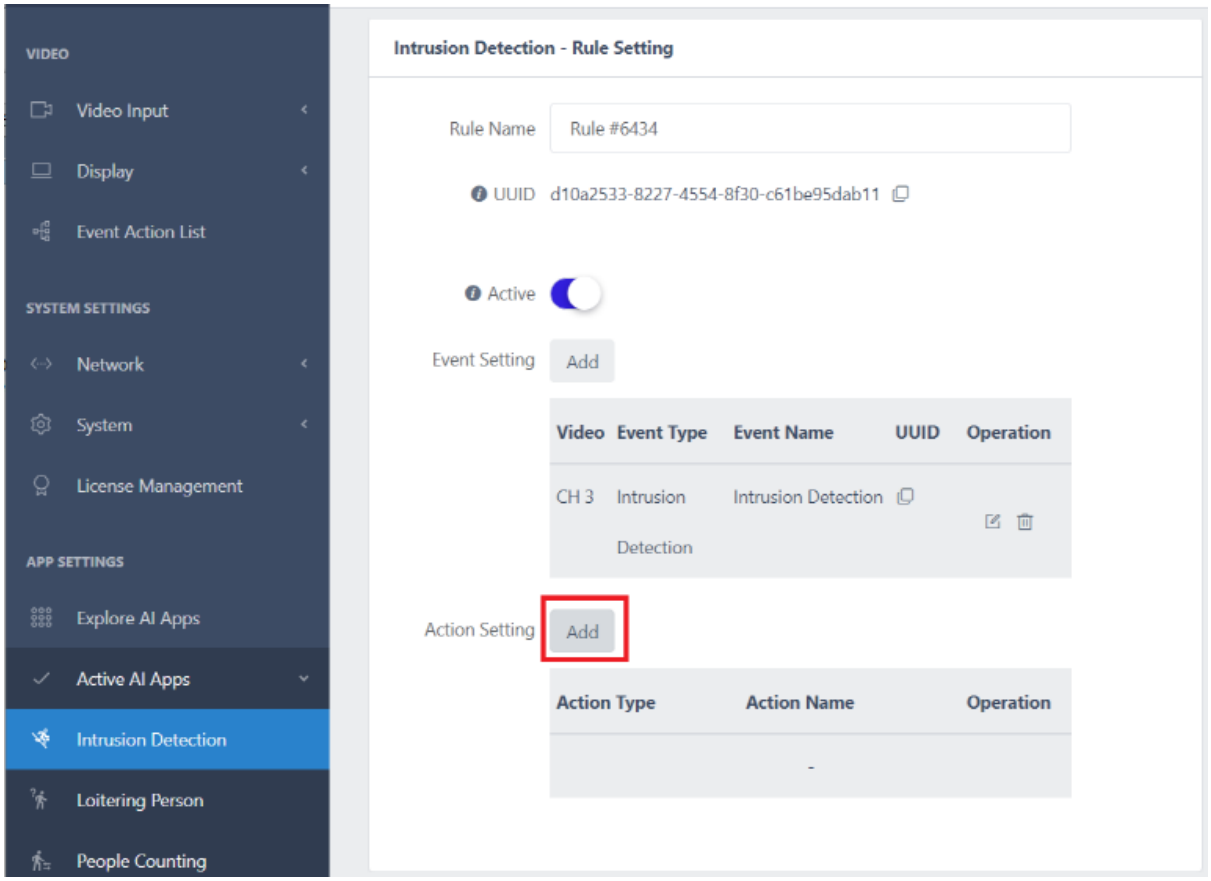
Set (add) the video stream. You can add it either by using an Onvif device search or by directly adding the IPCAM RTSP stream address.



2) Set up the AI App

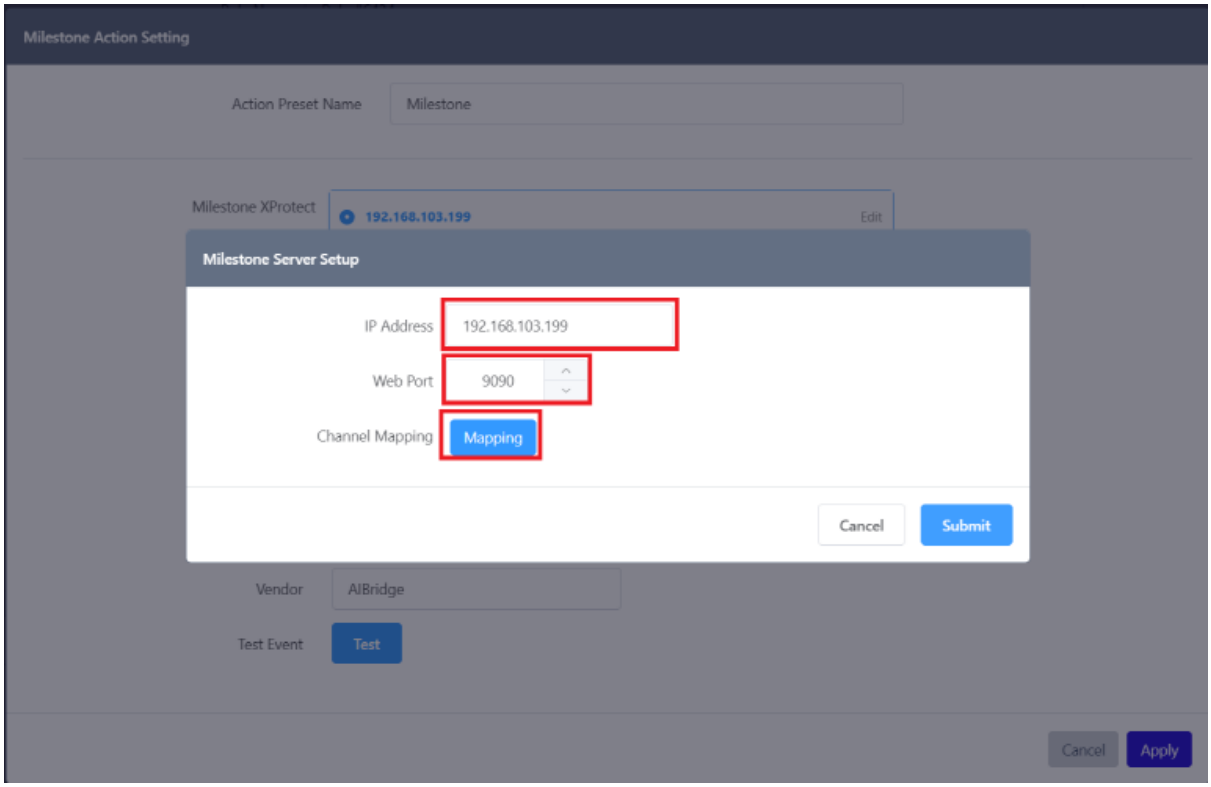
Select the desired AI App and set the AI event for the channel.

In the Actions Setting, click the Add button to add the Milestone action handler.



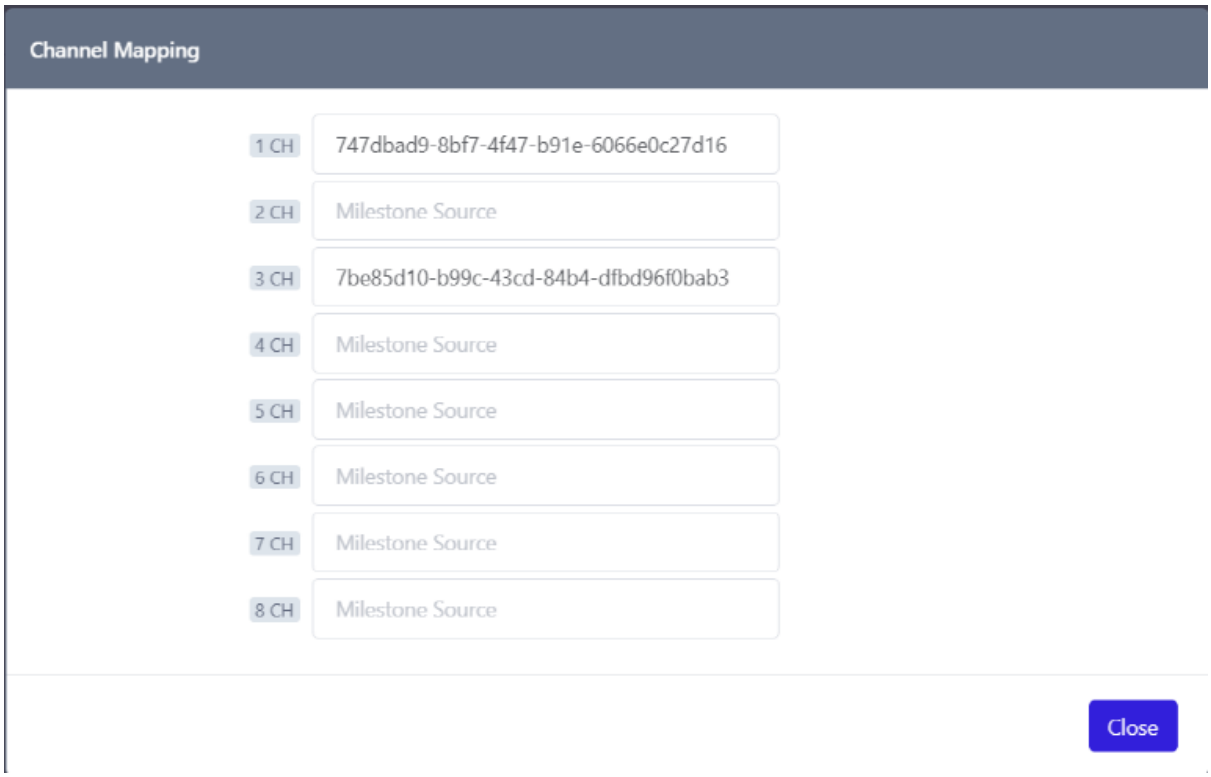
3) Enter the Milestone XProtect VMS Server Information

Enter the IP address of the Milestone XProtect VMS and the Analytic Event service port number. Then click the channel "**Mapping**" button.

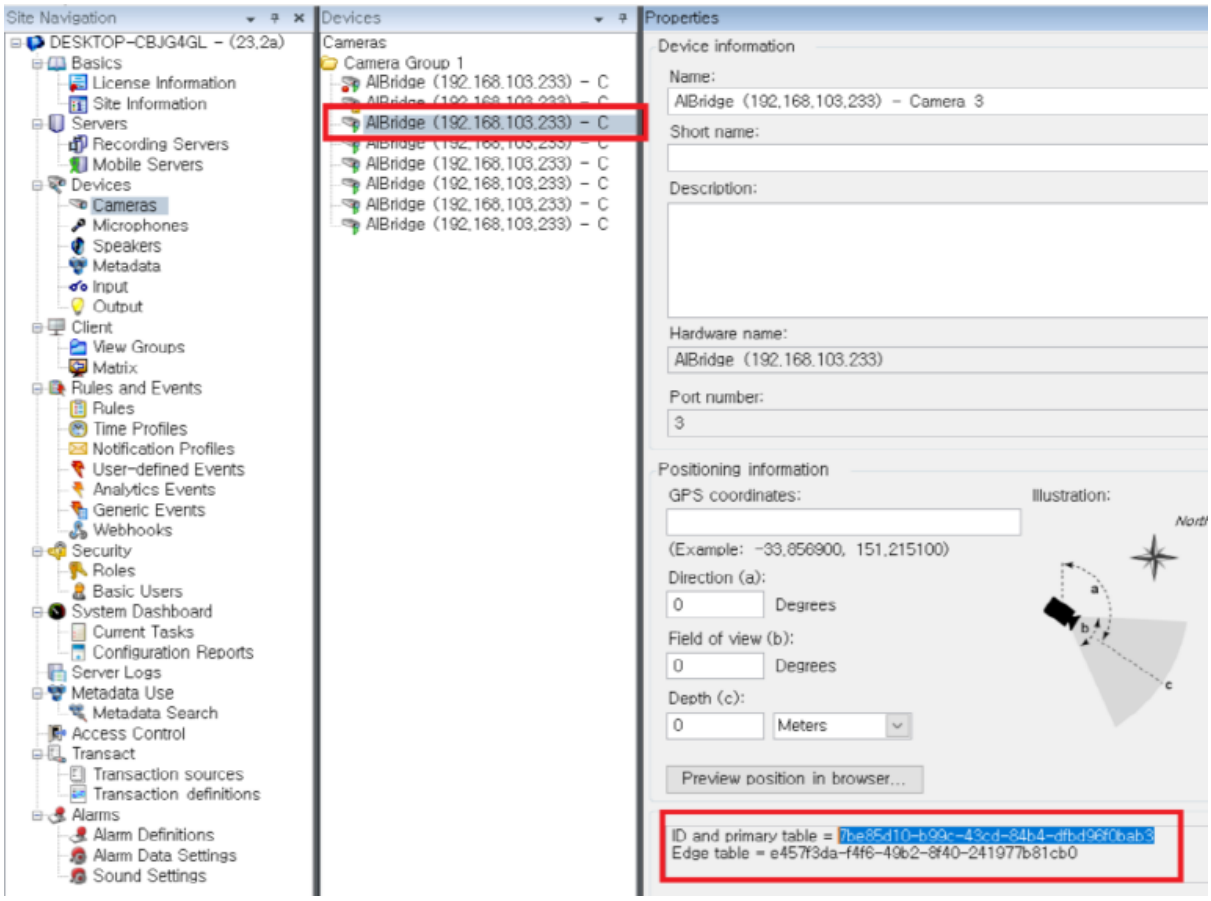


Enter the Camera Channel ID of Milestone XProtect VMS.

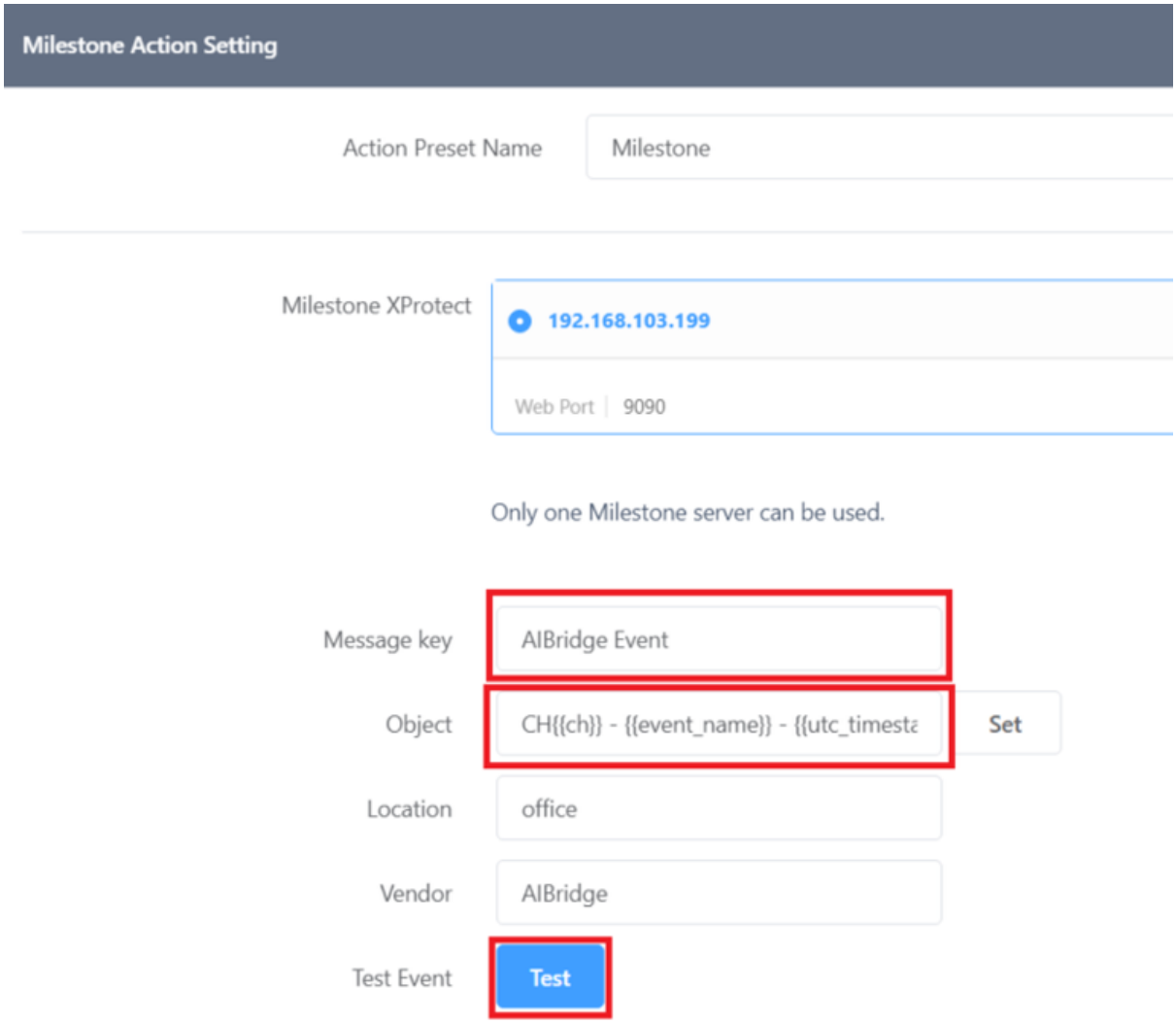
Note: If you enter the IPCAM channel ID information instead of the AIBOX camera channel ID in the camera mapping information, it operates as the Case2 integration type.



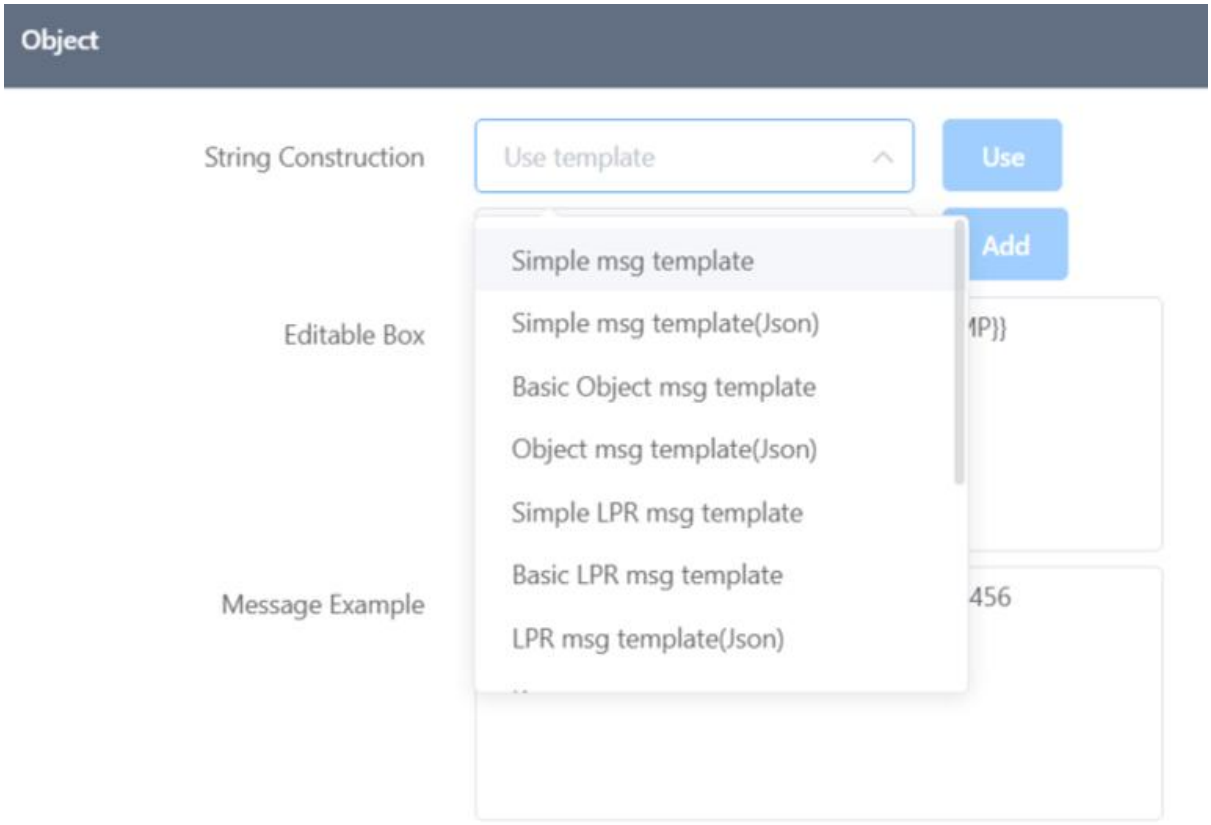
You can find the UUID for the Camera Channel ID by selecting the channel with the mouse while holding down the CTRL key and then looking at the bottom of the info tab.

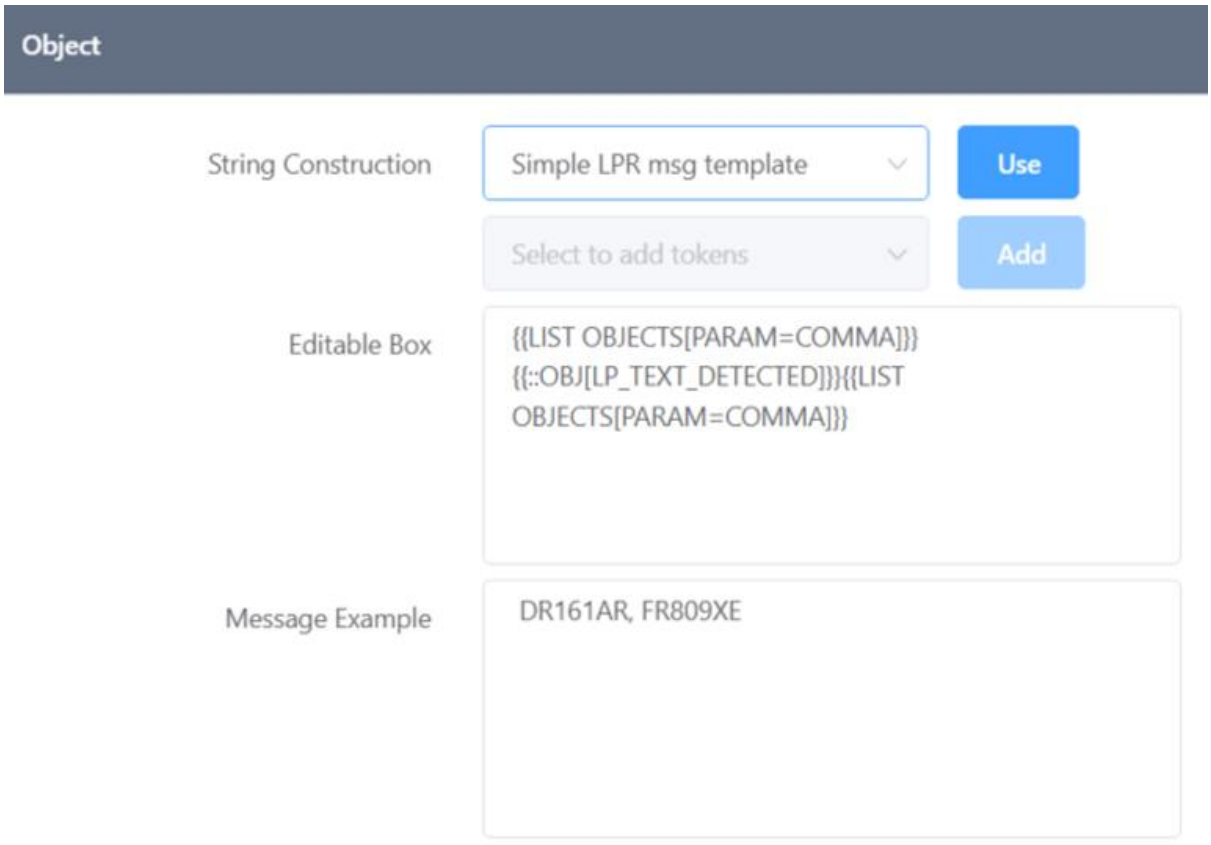


For the “Message Key” property, input the name of the “Analytic Event” that you added in Milestone XProtect. In this guide, we have entered it as “**AIBOX Event**“.



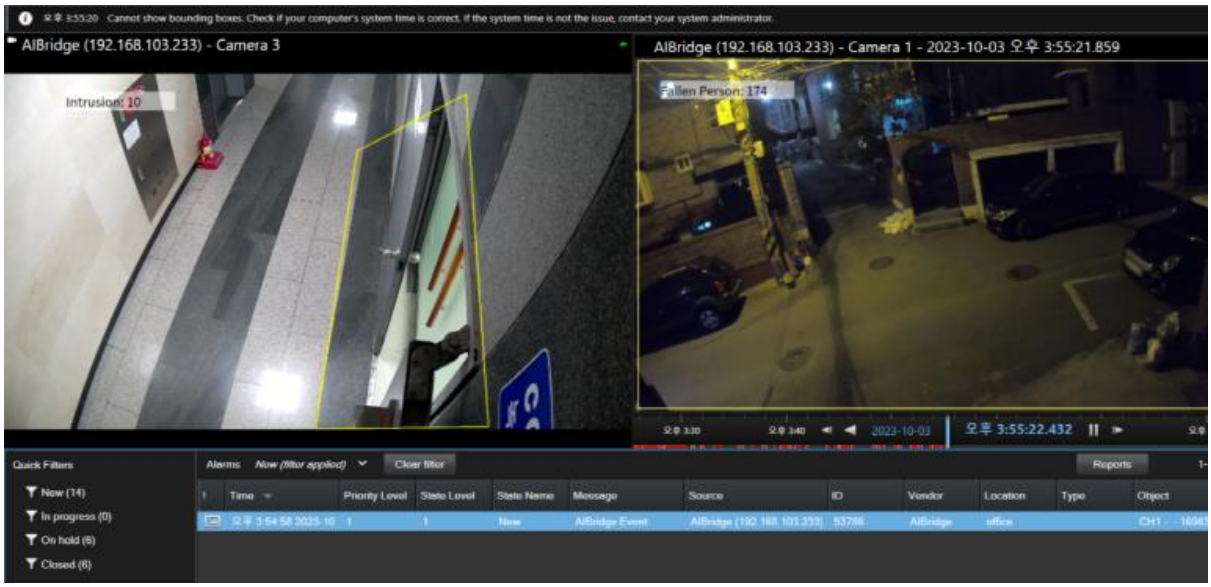
The Object field can be utilized in various ways. You can enter event texts, LPR information, etc., so you can send additional information in the Milestone XProtect Alarm Manager.



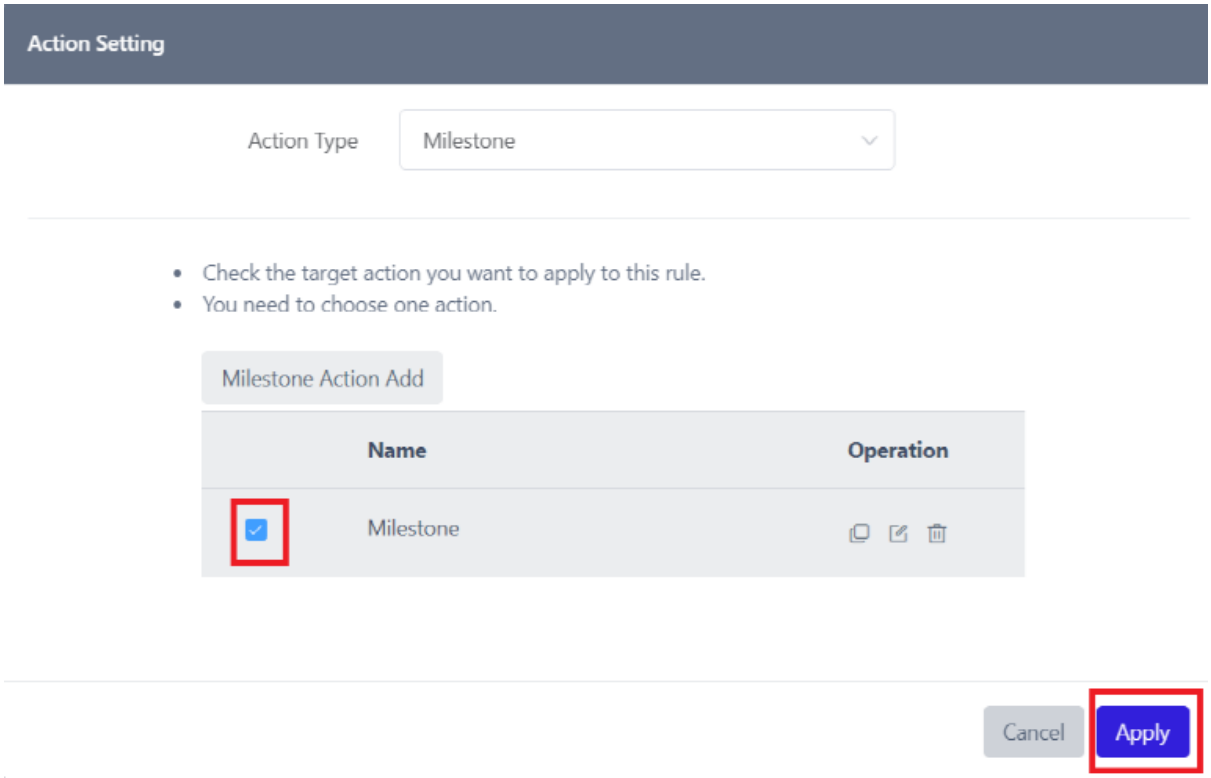


Note: If you want to set the Object property differently for each AI App, you can create a separate Milestone Action handler for each AI App.

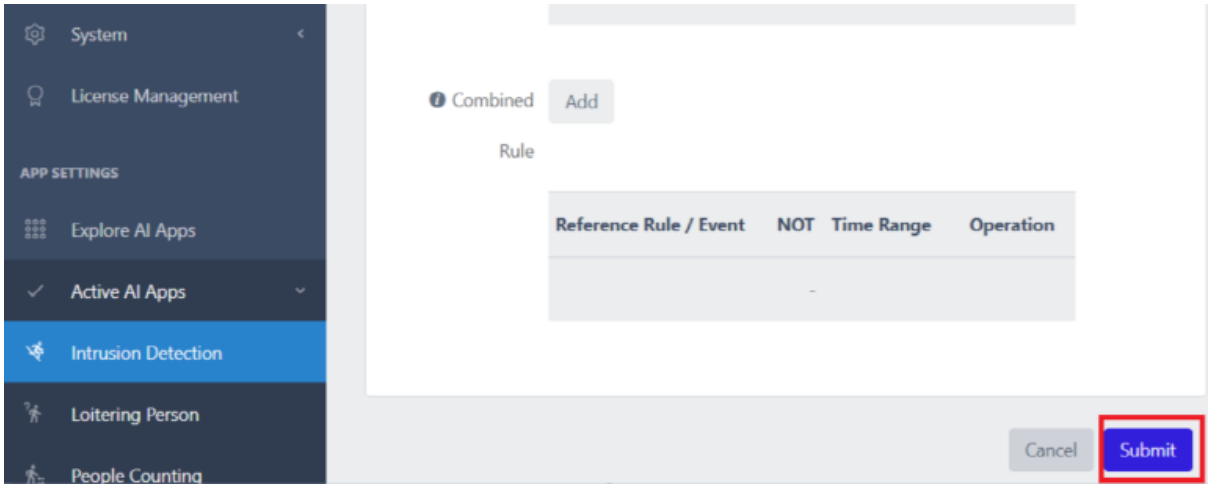
By pressing the “Test” button, you can check the Test Event in the Milestone XProtect Client.



If the event test is successful, check the “Activate Milestone action handler” checkbox and press the “Apply” button to save the handler settings.



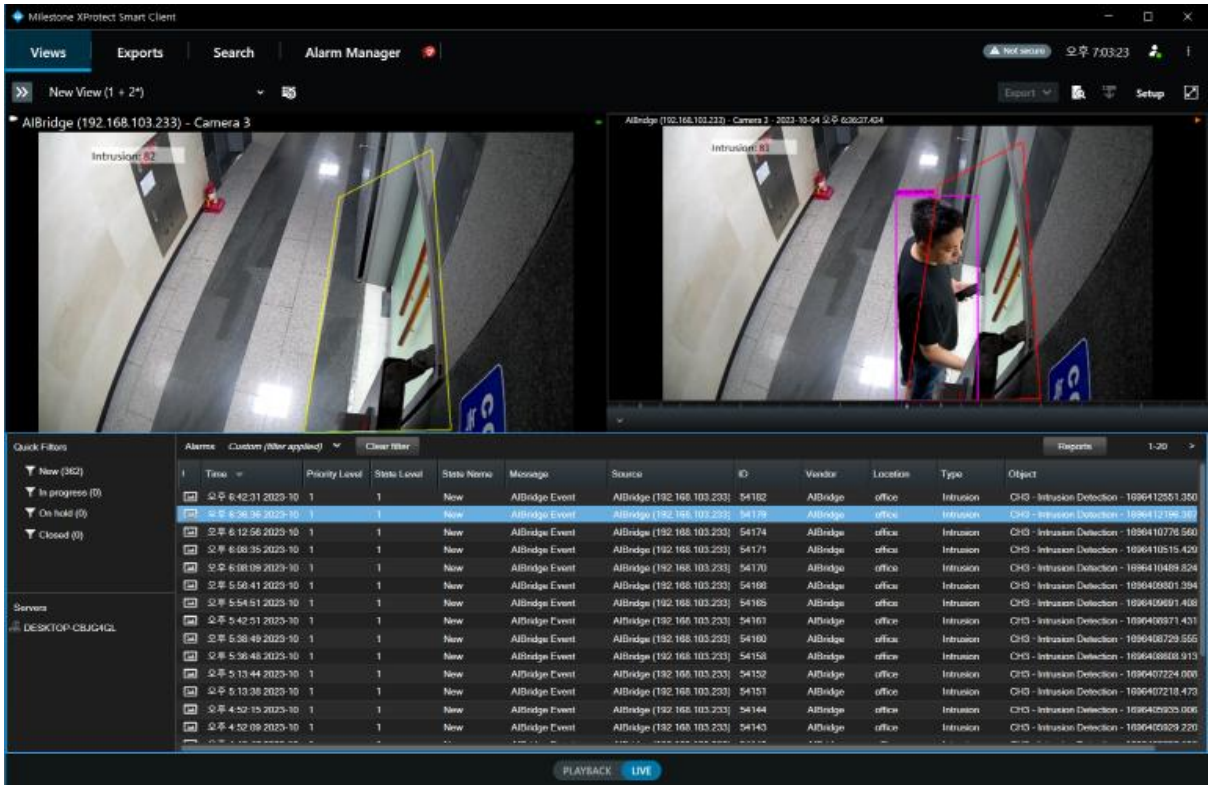
Finally, press the “Submit” button located at the bottom of the AI App settings to save all configurations.



3. Demo

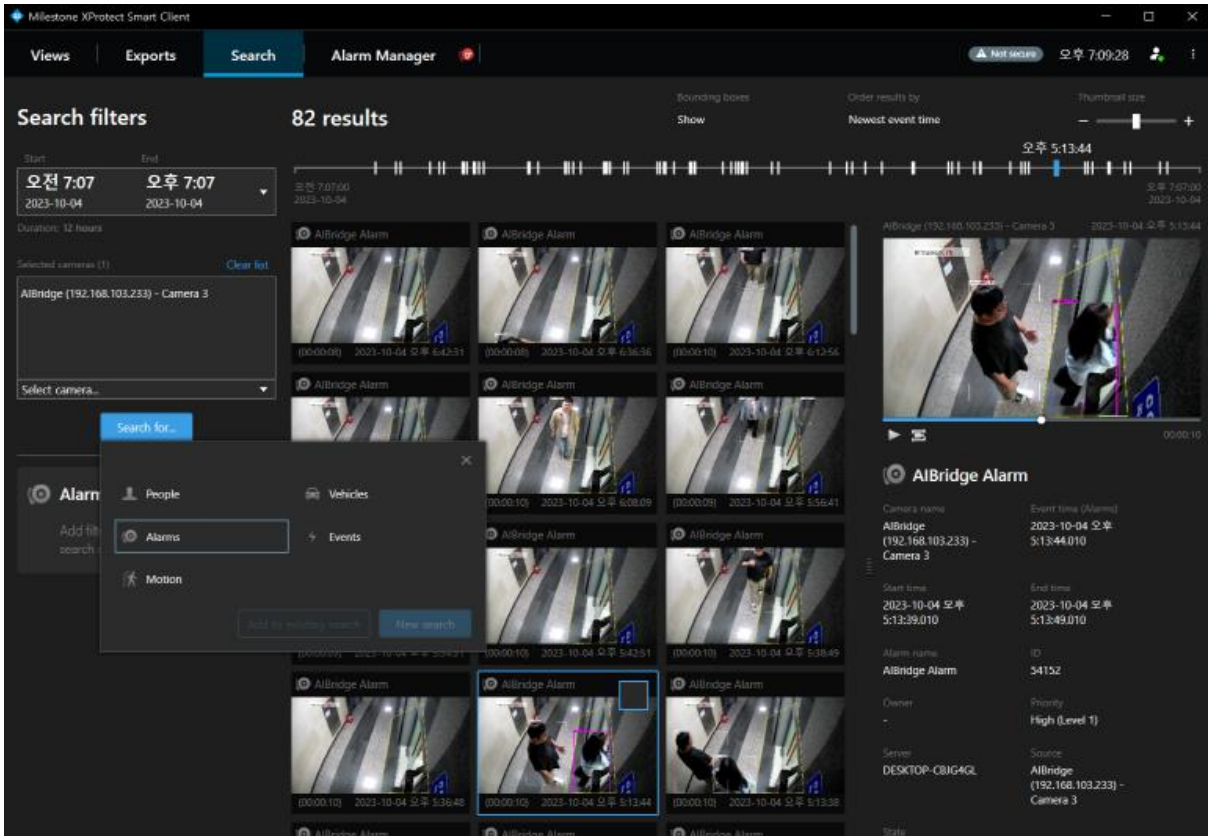
3.1 Live

In the Live screen of the XProtect Smart Client, the analytics events will be listed within the Alarms panel as well as the annotated video.



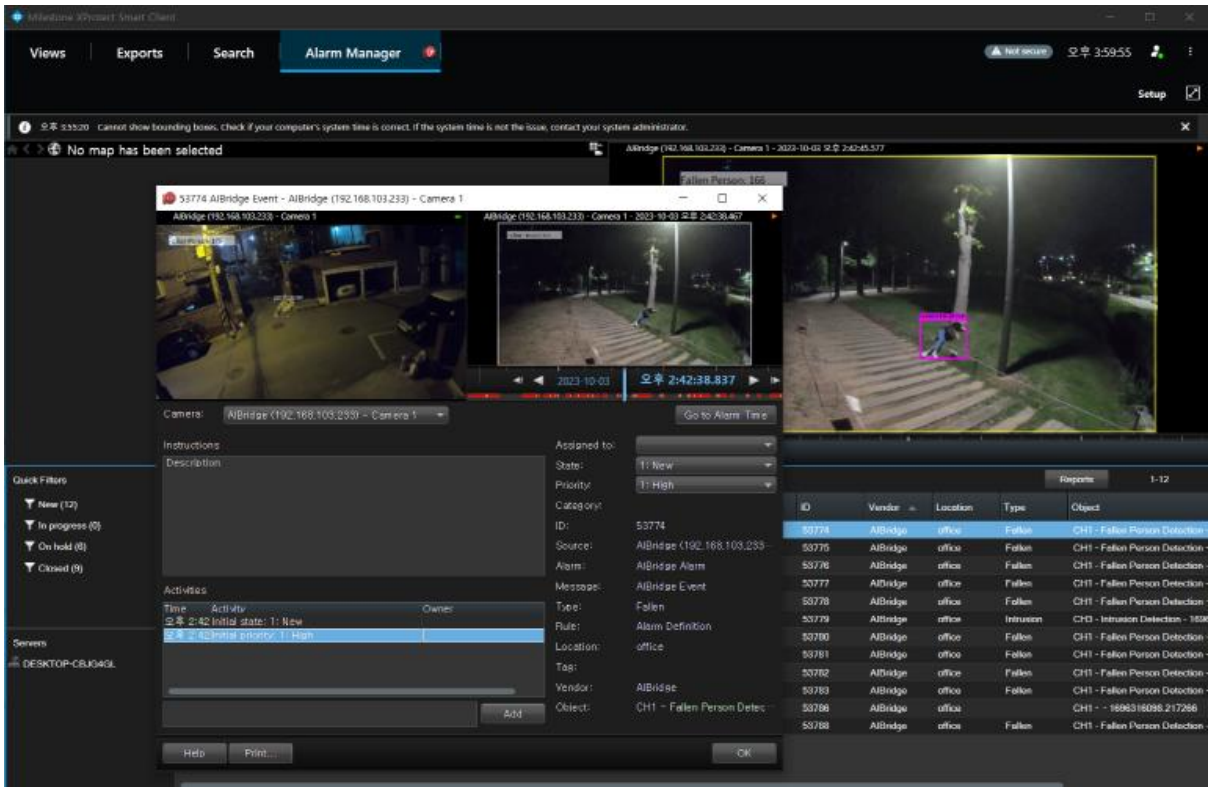
3.2 Search

In the search menu, click on the “Search for..” button and select Alarms to search for AI Events.



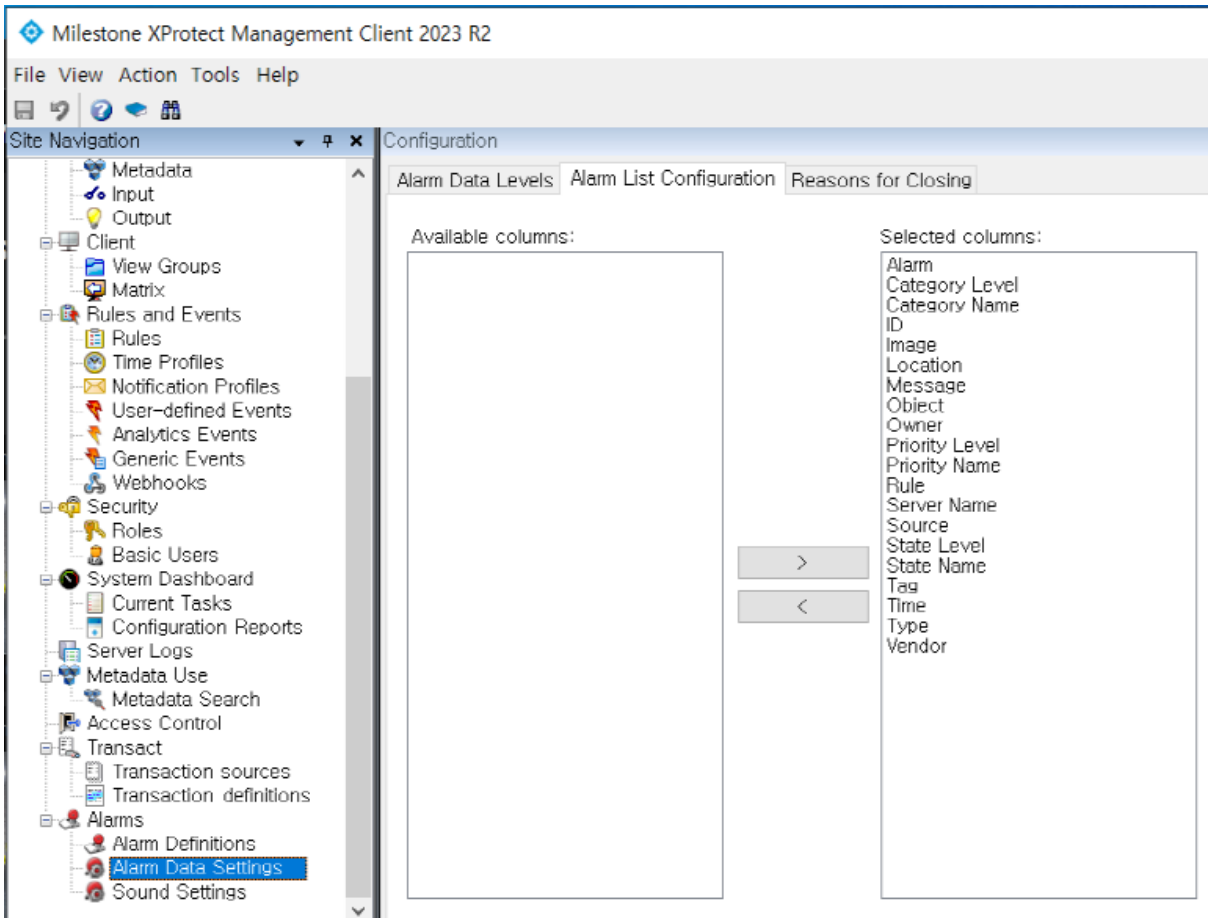
3.3 Alarm Manager

In the Alarm Manager, by clicking on an individual alarm, you can check detailed event occurrence information with recorded video.

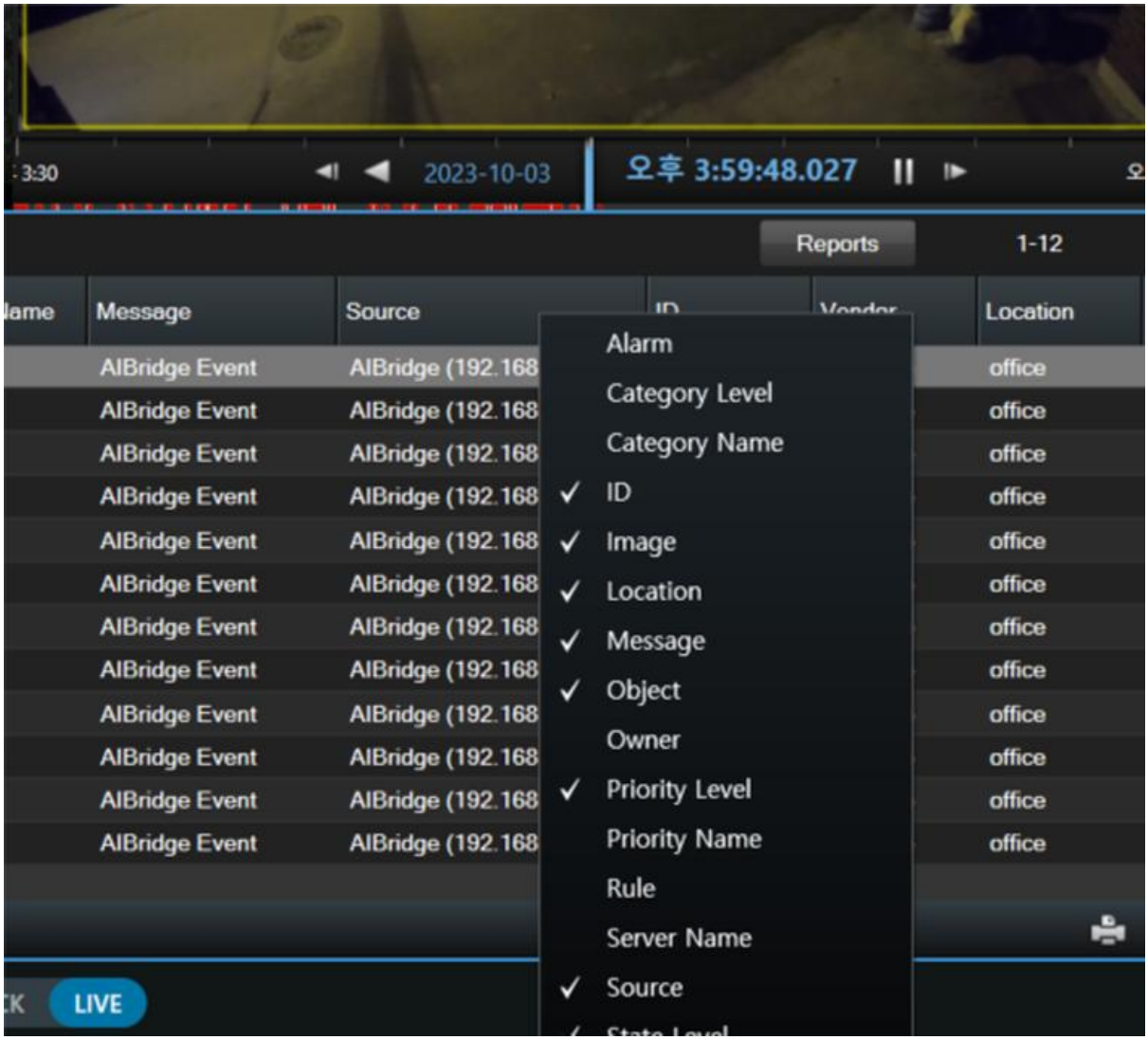


Note: The Alarm Manager is supported in Milestone XProtect Express+ and higher versions.

To display analytic event properties in the Smart Client, you might need to adjust settings in the Management Client. First, navigate to “Alarms” and then to “Alarm Data Settings”. From there, choose the event properties you want and transfer them from the left panel to the right.



To display the event properties in the Smart Client, right clicking on the event header and select the fields to display



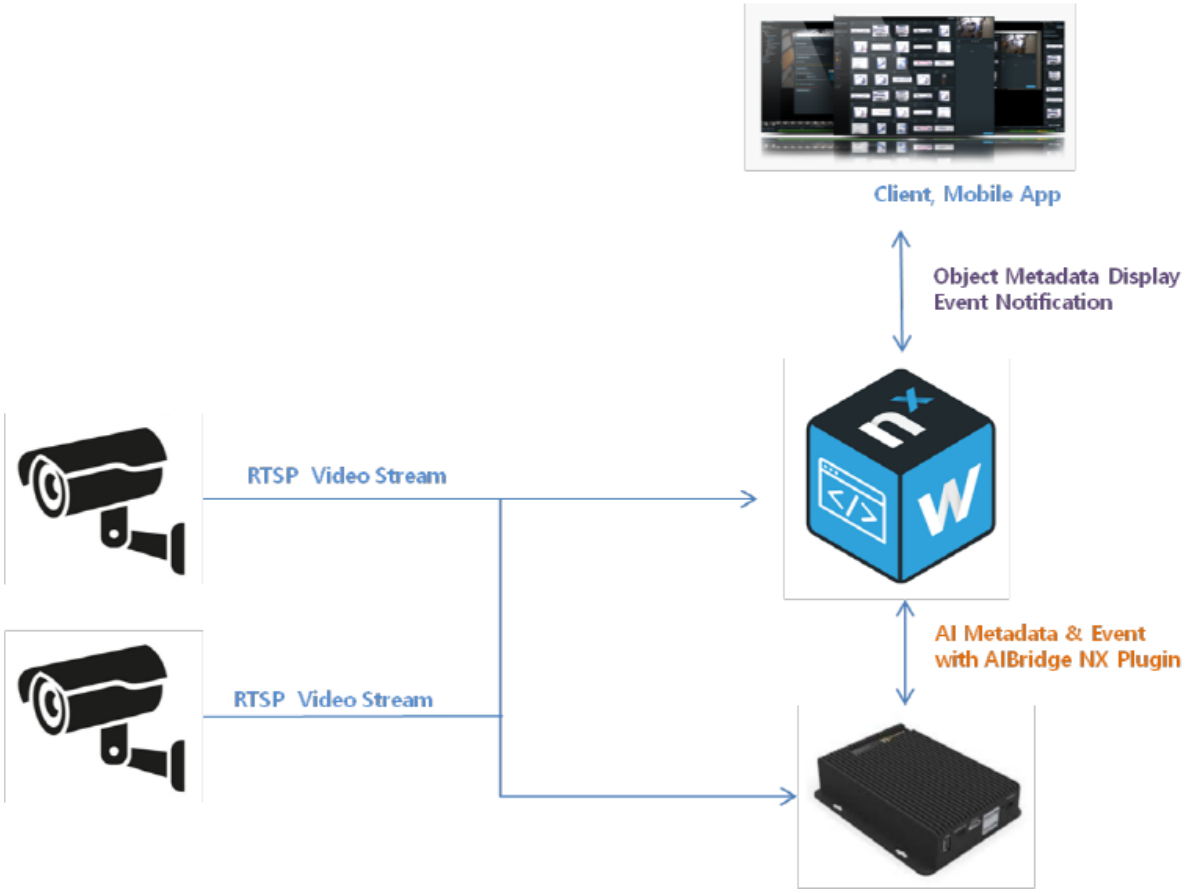
Network Optix Integration Guide

1. Introduction

1.1 Prerequisites

- AIBOX FW version 10137 or greater.
- Network Optix Witness VMS version 4.2.0.32840 or greater.
- Network Optix Witness VMS version 5.0.0.35745 or greater.
- Network Optix Witness VMS version 5.1.0.37466 or greater.

1.2 Learn about integration architecture



- IP Camera transmits video stream to NX VMS and AIBOX.
- AIBOX analyzes the received video stream by AI Apps.
- AIBOX sends metadata & event to NX VMS with AIBOX NX Plugin.

2. AIBOX NX VMS Plugin Install & Configuration

2.1 Install Nx Witness VMS

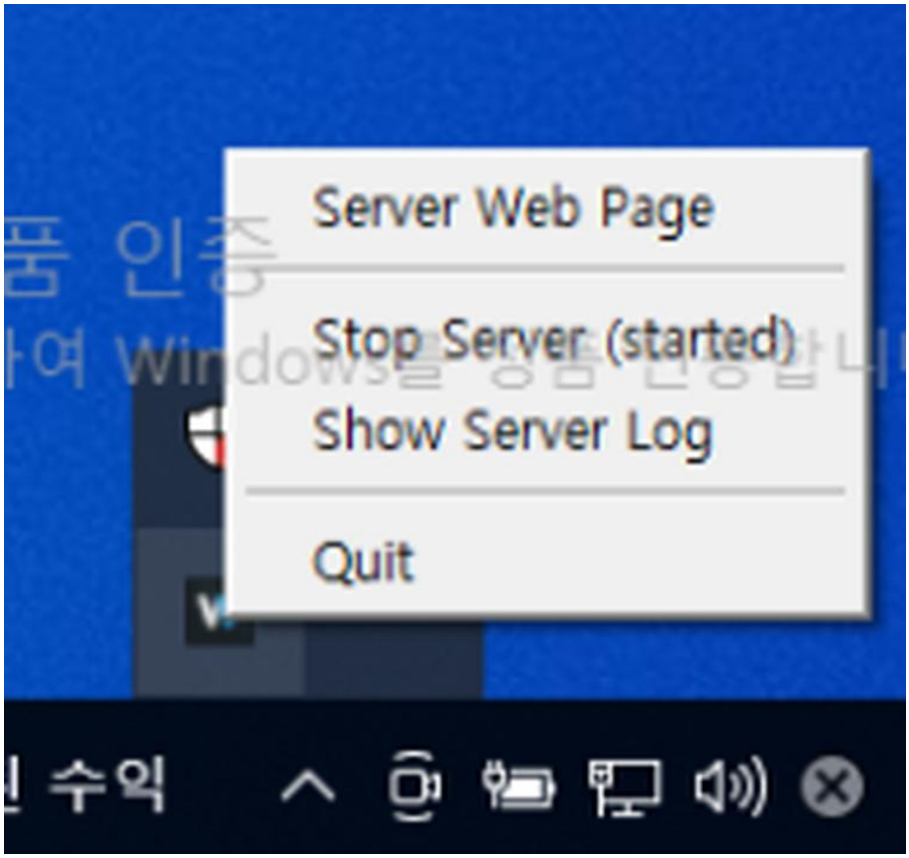
Install the Nx Witness VMS v5.X or later. You will need both Server and Client, as the Client will be used in configuration.

2.2 Install AIBOX Plugin

(On Windows)

Stop the Nx Witness server

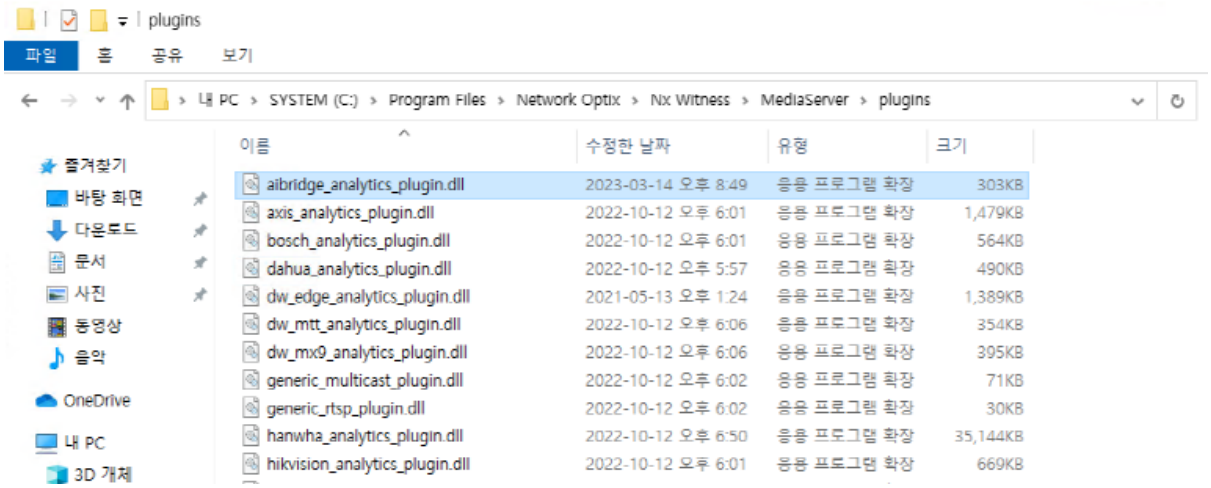
By right-clicking the tray icon and selecting Stop Server.



Download the AIBOX analytics plugin from our Customer Portal and unzip.

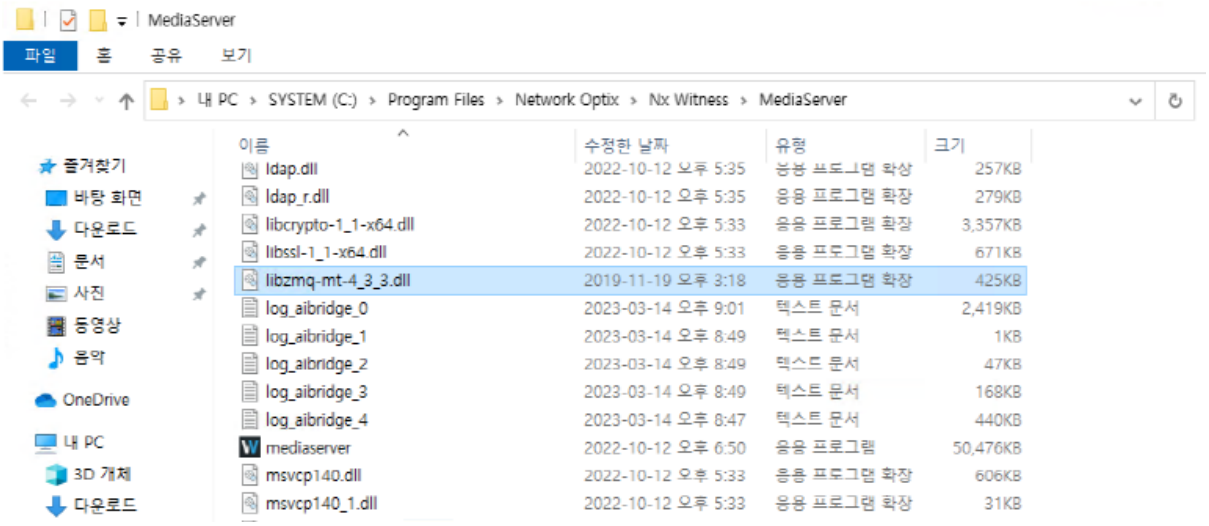
Copy the “**AIBOX_analytics_plugin.dll”** file to {NxInstallPath}\plugins\ usually on

“C:\Program Files\Network Optix\Nx Witness\MediaServer\plugins”.



Copy the **libzmq-mt-4_3_3.dll** file to {NxInstallPath}\ usually on

“C:\Program Files\Network Optix\Nx Witness\MediaServer\”.

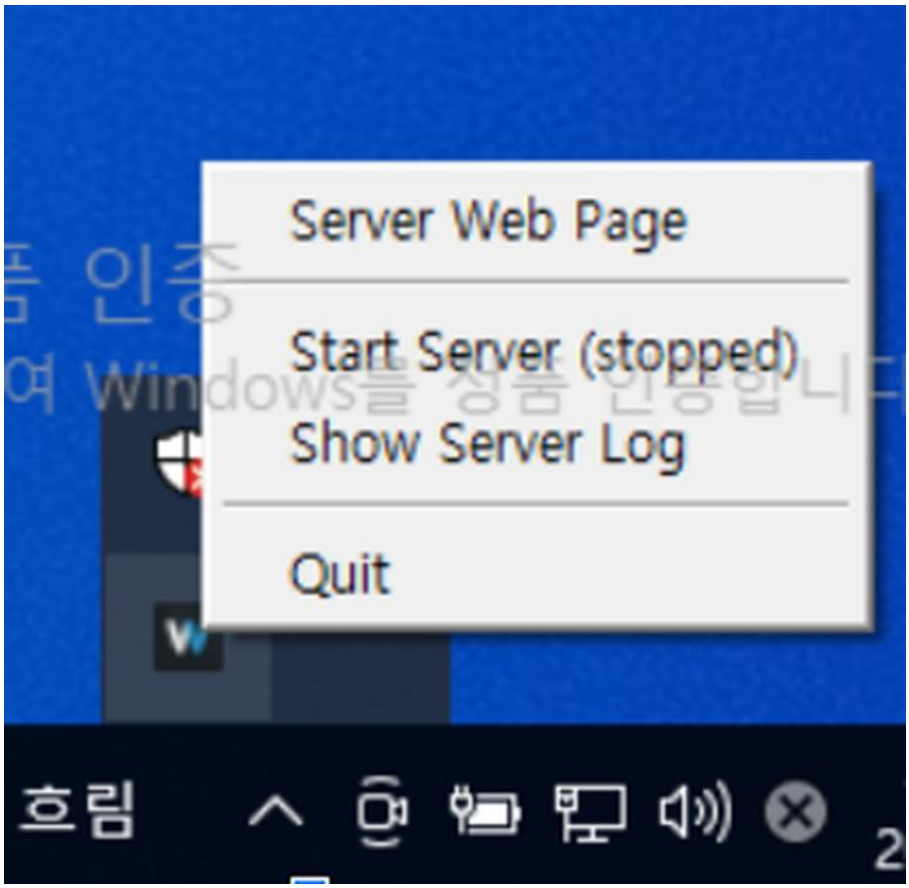


Download & Install vc_redist.x64.exe

(https://aka.ms/vs/16/release/vc_redist.x64.exe)

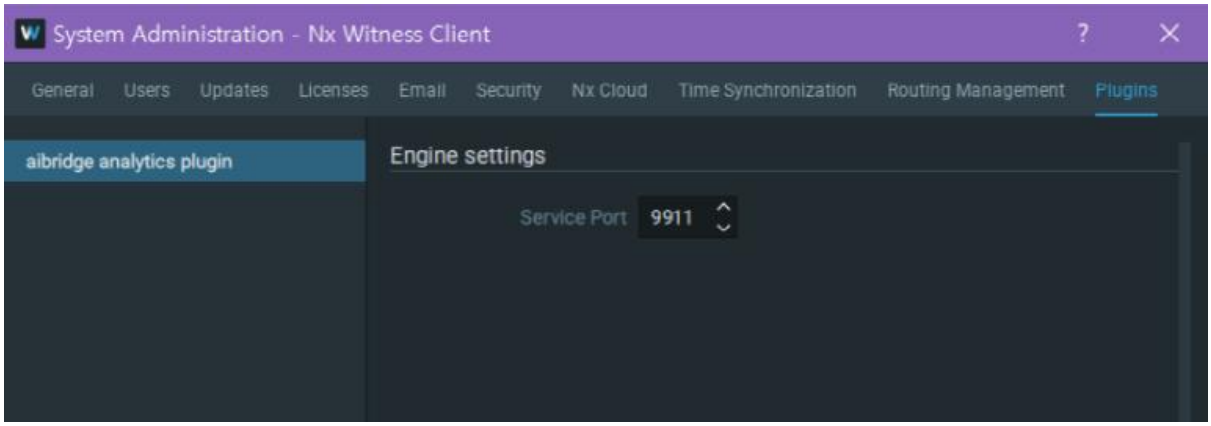
Start the Nx Witness server

By right-clicking the tray icon and selecting Start Server.



Setup communication port & Setup Firewall

In the AIBOX analytics plugin engine setting menu, (Network Optix VMS System Administration > Plugins Menu) set a unique port (**9911**) . This is a TCP port which is used for a communication between the Nx Witness AIBOX analytics plugin and AIBOX.



If your Windows is using a firewall, add New Rule in Windows Firewall Setup > Advanced Settings > Inbound Rules > New Rule.

Note) How to Add a Rule or Port to a Windows 10 Firewall

https://www.youtube.com/watch?v=JsEulhg5P8k

(On Linux – Ubuntu x64 18.04, 20.04, 22.04)

Download the AIBOX analytics linux plugin from our Customer Portal and please enter the following commands in order.

tar zxvf AIBOX_plugin_v1.1.0_20230808.tar.gz

cd AIBOX_plugin_v1.1.0_20230808

chmod 755 install.sh

sudo ./install.sh

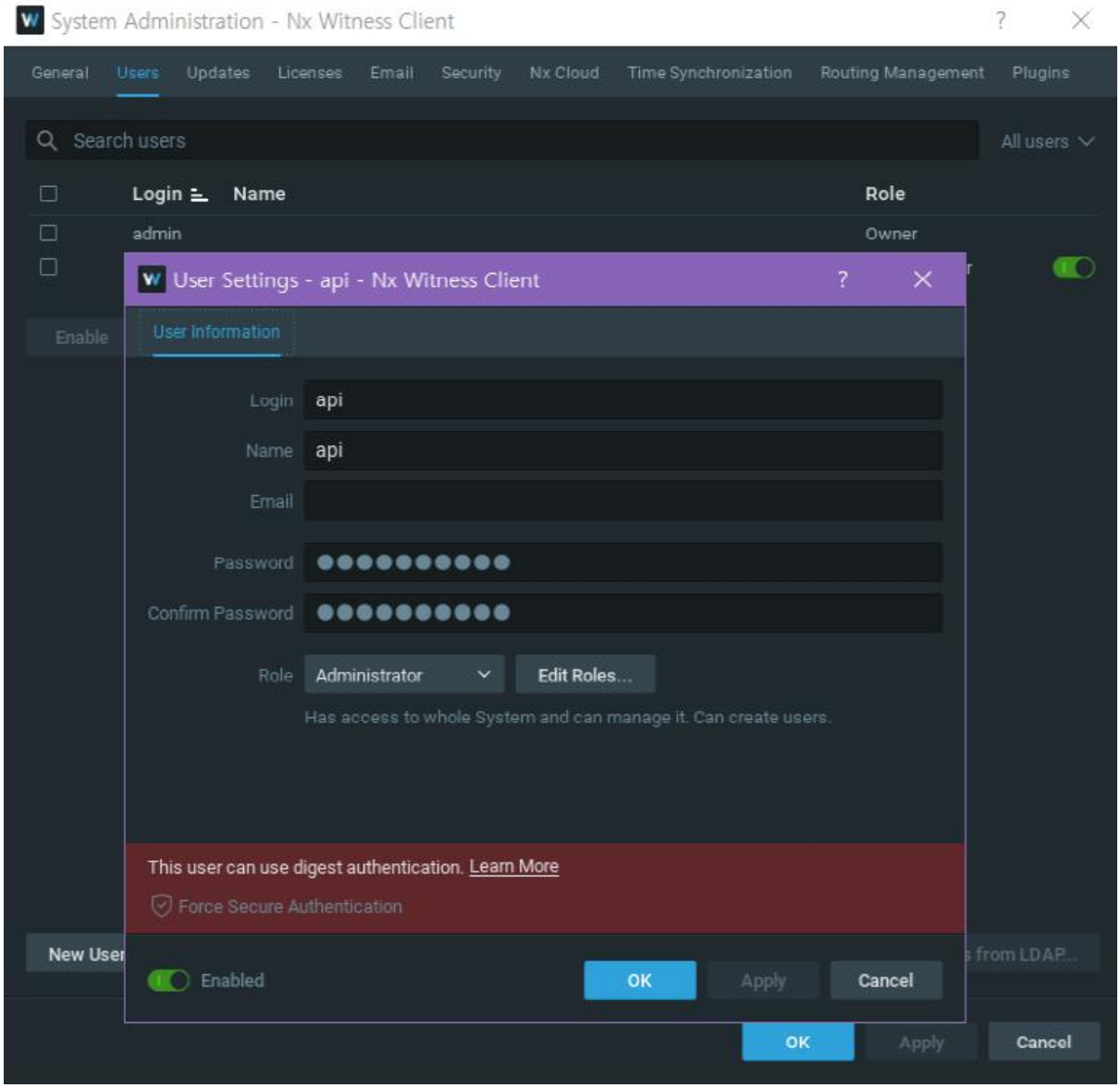
```
build@build-dev1804:/tmp/aibridge_plugin_v1.1.0_20230808$ sudo ./install.sh
[sudo] password for build:
Do you want to install aibridge_analytics_plugin? (y/n): y
The libzmq5 package is already installed.
The libboost-system1.65.1 package is already installed.
Copying libaibridge_analytics_plugin.so to /opt/networkoptix/mediaserver/bin/plugins
Restarting networkoptix-mediaserver service
Installation completed successfully.
Do you want to restart the networkoptix-mediaserver service? (y/n): y
Restarting networkoptix-mediaserver service
● networkoptix-mediaserver.service - Network Optix Media Server
   Loaded: loaded (/etc/systemd/system/networkoptix-mediaserver.service; enabled; vendor preset:
   Active: active (running) since Tue 2023-08-08 15:00:46 KST; 1s ago
  Process: 18698 ExecStartPre=/opt/networkoptix/mediaserver/lib/scripts/systemd_mediaserver_pre_s
 Main PID: 18701 (mediaserver)
    Tasks: 40 (limit: 8191)
   CGroup: /system.slice/networkoptix-mediaserver.service
           ├─18665 /usr/bin/pulseaudio --start --log-target=syslog
           └─18701 /opt/networkoptix/mediaserver/bin/mediaserver -e --crash-directory=/opt/networ
```

note) By executing the install.sh script, it automatically detects the Ubuntu OS version and NX Witness, NX MetaVMS, and installs the necessary packages automatically. Follow the instructions in the script to install the module, and restarting the VMS will complete the plugin installation

2.3 Add NX api Account

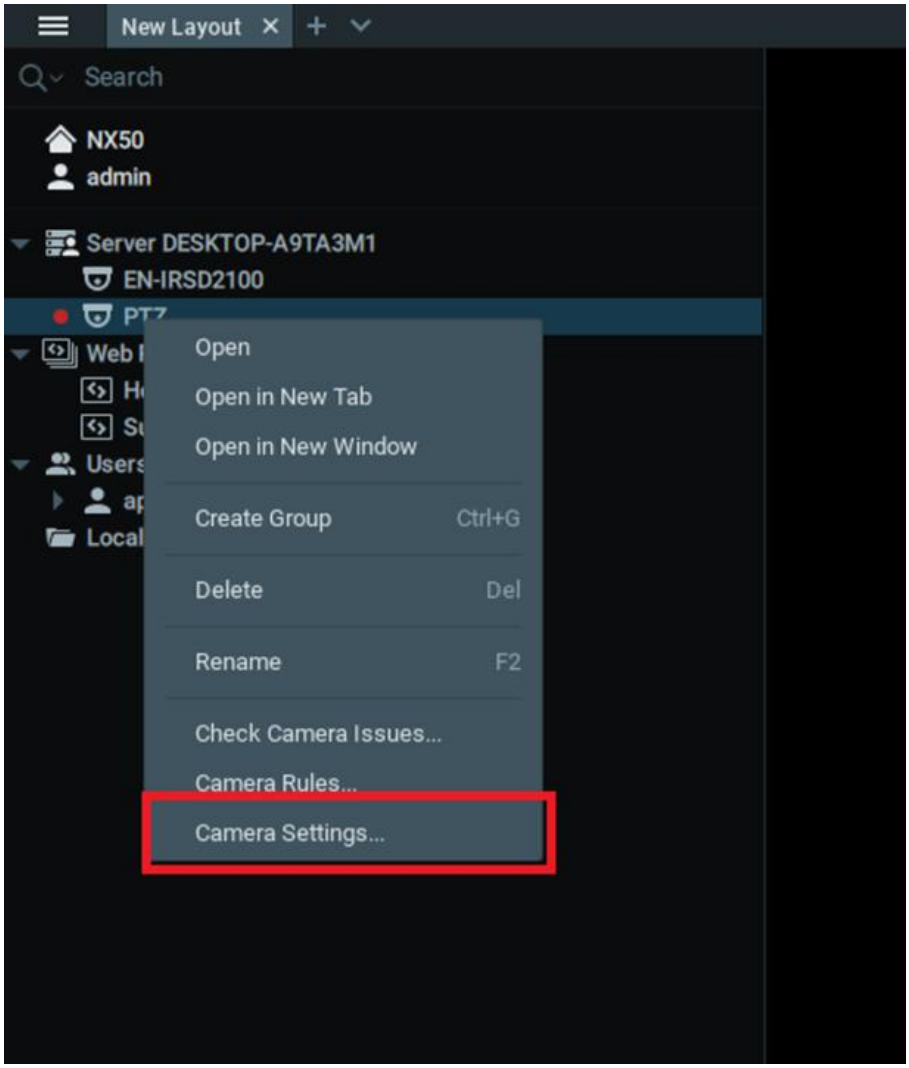
Add NX “api” account to be used by AIBOX.

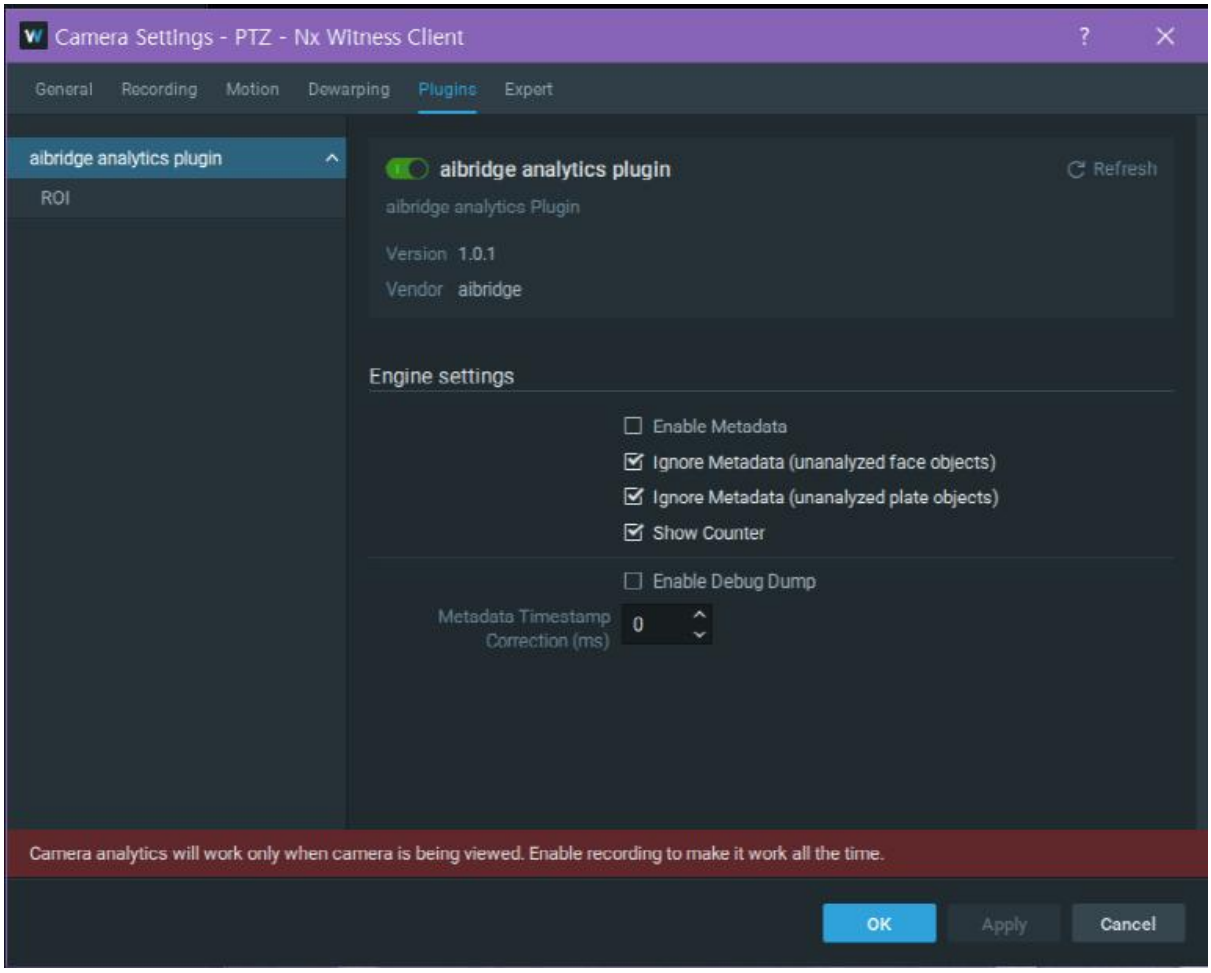
When creating an account, **enable digest authentication and set the administrator rol**e.



2.4 Enable video channels to use AIBOX analytics plugin

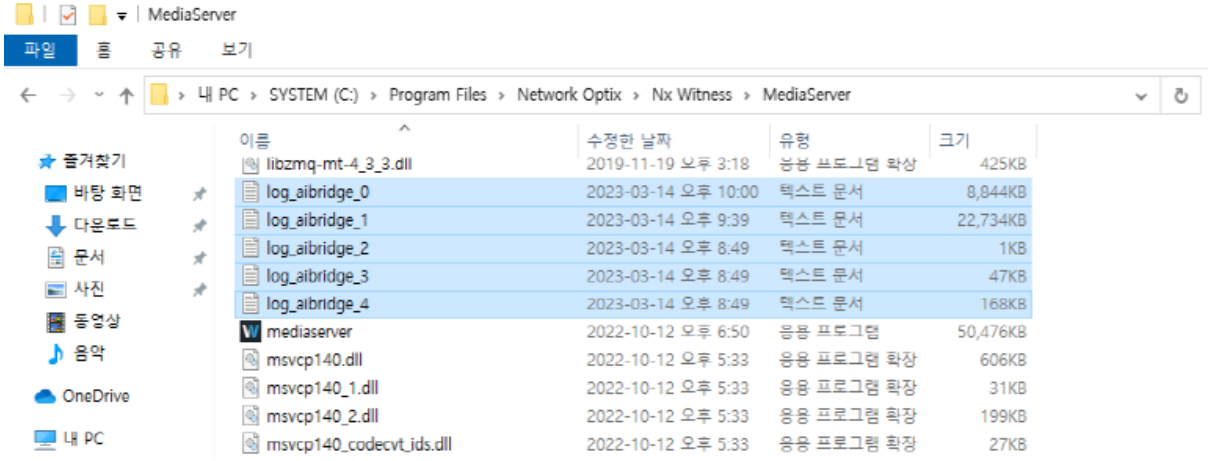
In the NX client left panel, right-click the camera you want to process with AIBOX and select Camera Settings. In the Plugins tab, enable the AIBOX analytics plugin.


New Layout
Search
NX50
admin
Server DESKTOP-A9TA3M1
EN-IRSD2100
Open
Open in New Tab
Open in New Window
Create Group Ctrl+G
Delete Del
Rename F2
Check Camera Issues...
Camera Rules...
Camera Settings...



1. Enable Metadata : **It is not recommended to use it except for installation or debugging purposes.** Even if this option is disabled, the object on which the event occurred is automatically displayed (saved).
2. Ignore Metadata (unanalyzed face objects) : Face information that has not been analyzed is ignored.
3. Ignore Metadata (unanalyzed plate objects) : plate(LPR) information that has not been analyzed is ignored.
4. Show Counter : show number of Event Occurred.
5. Enable Debug Dump : **It is not recommended to use it except for installation or debugging purposes**. A large size of log files can be stored in the {NxInstallPath}\ usually on “C:\Program Files\Network

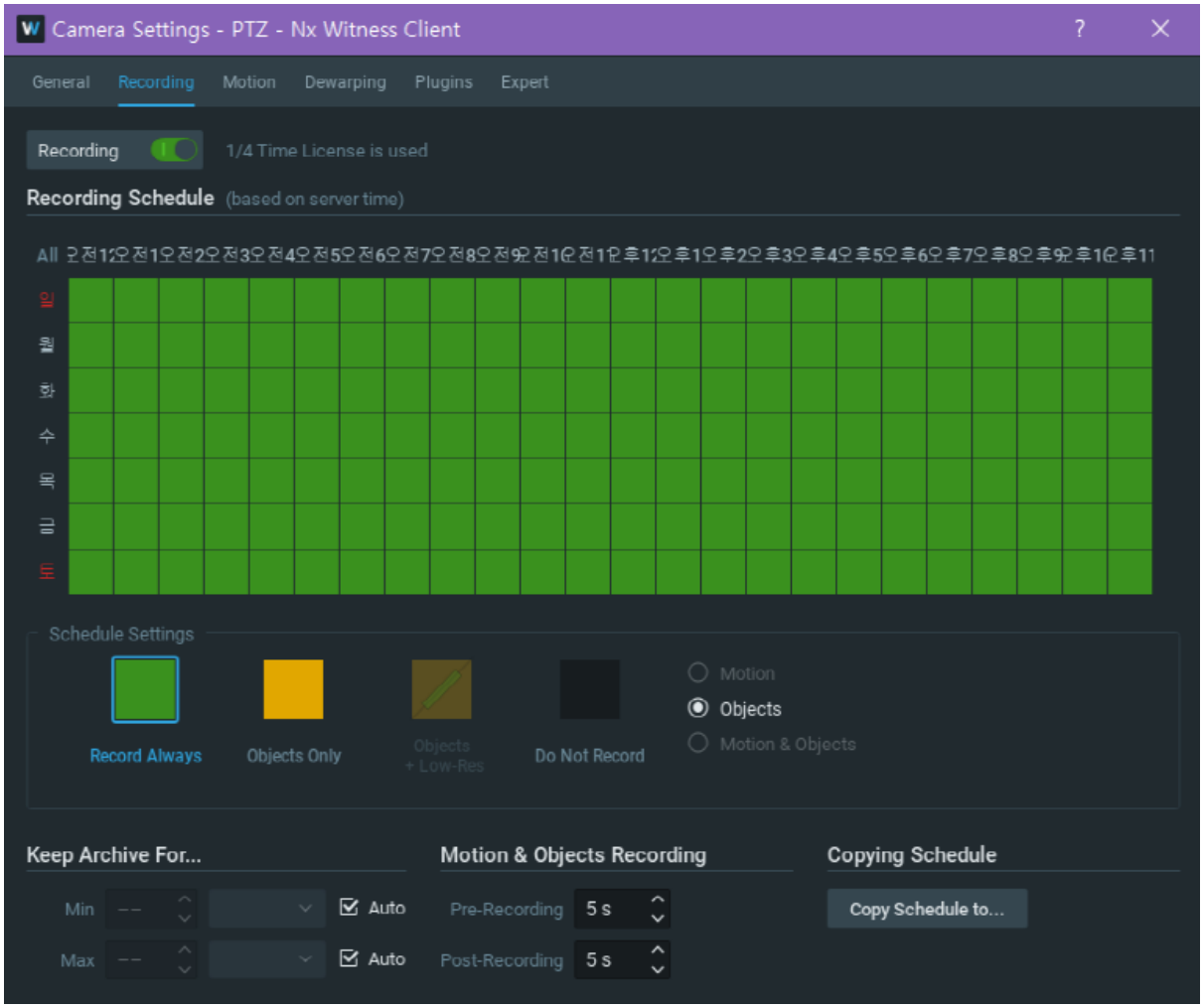
Optix\Nx Witness\MediaServer\". **It should be disabled in a production environment.**



6. Metadata Timestamp correction : Metadata (bounding box) is buffered for the set time. (Metadata is displayed delayed for the set time.)
   If you want to resolve the delay, please refer to section 4.1.

2.5 Enable video channel recording

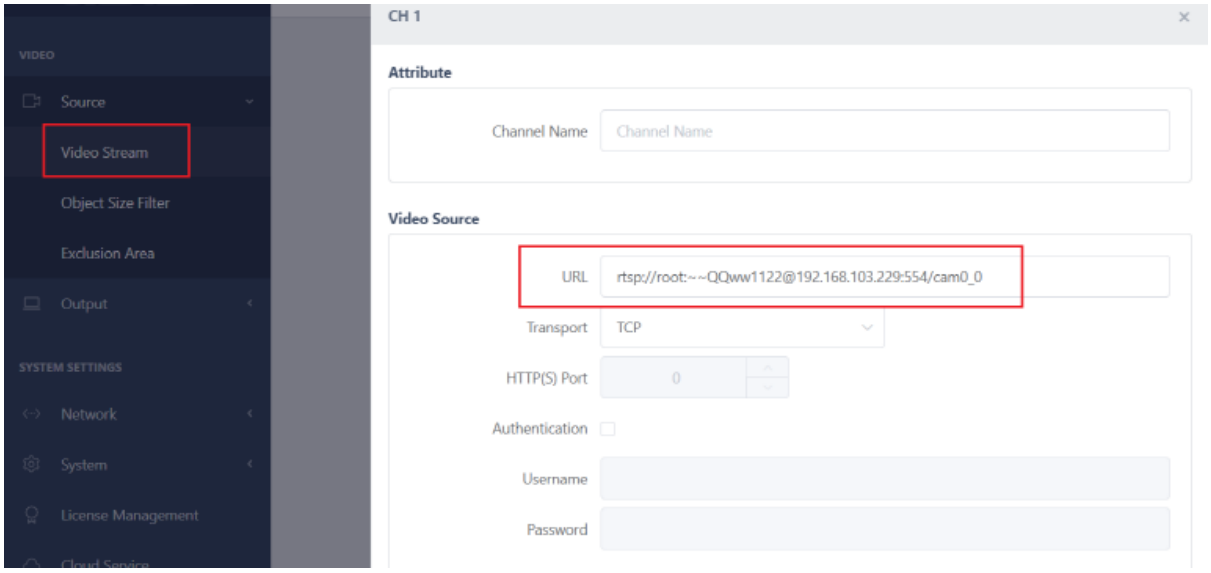
Non-recording analysis channels cannot use the EVENT and OBJECT panel in NX VMS.



3. AIBOX Configuration

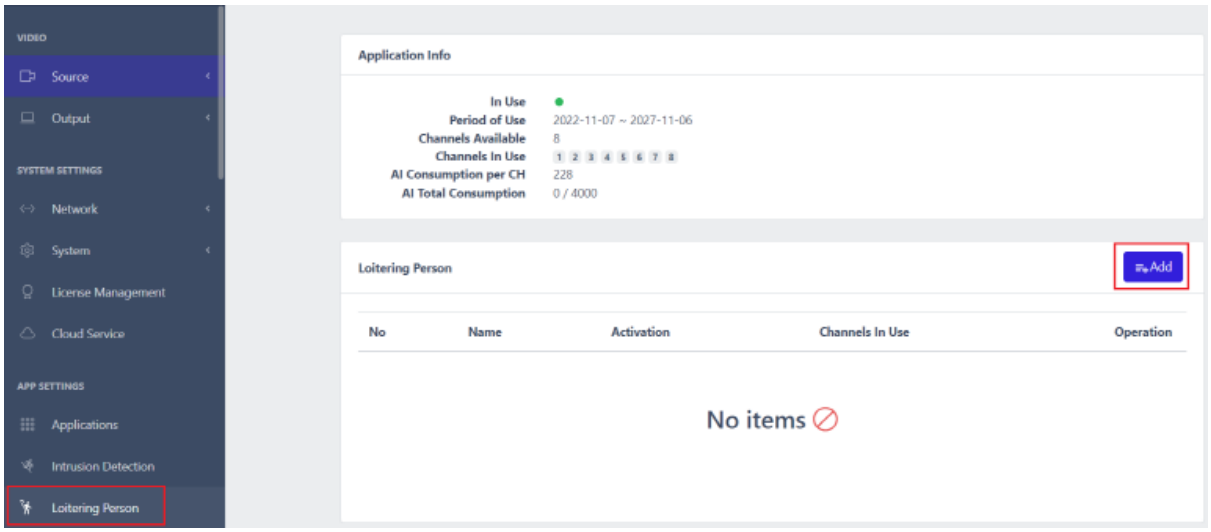
Let’s set up to integrate the Loitering Person app with the AIBOX Nx VMS Plugin.

3.1 Setting the video source

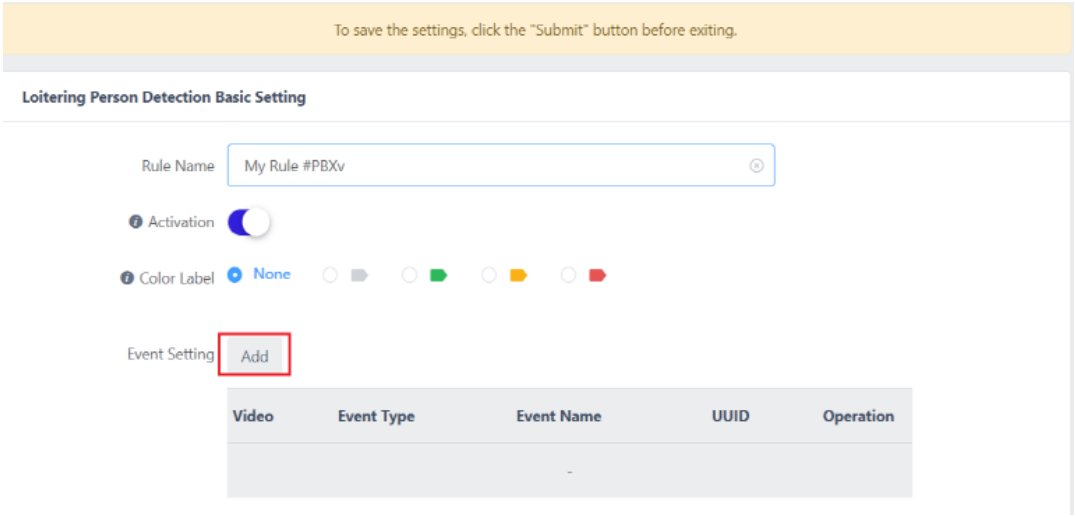


3.2 Setting up the Loitering Person app

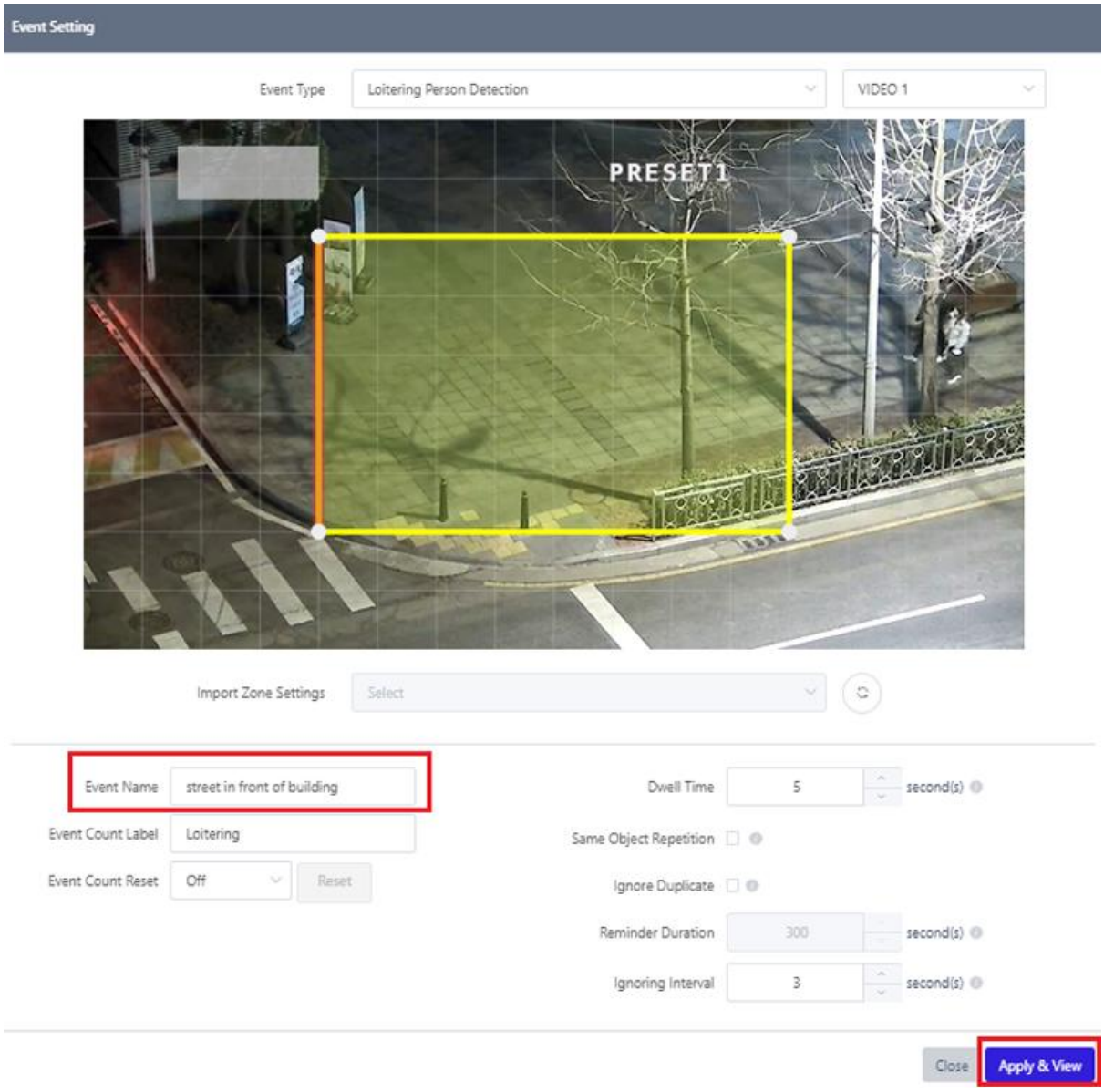
Add Rule



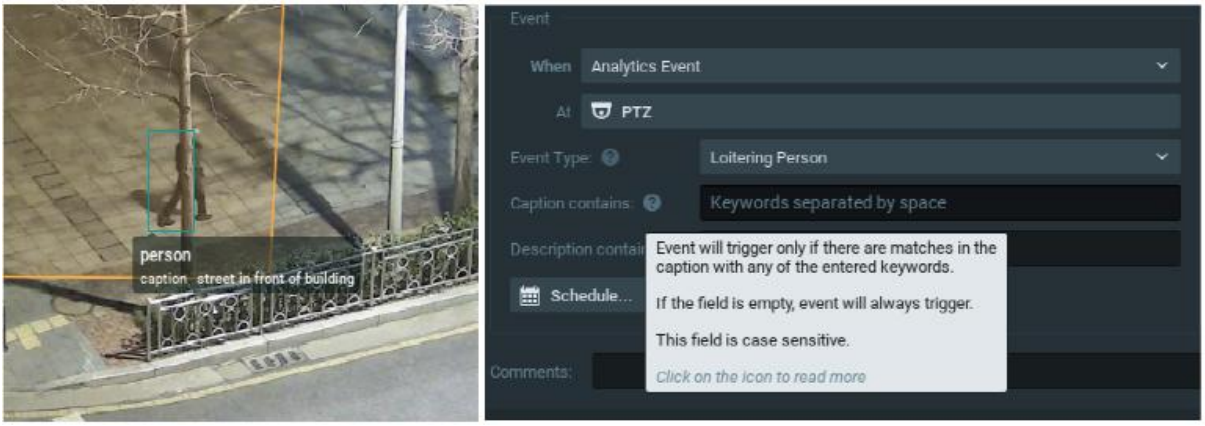
Adding event video source



Setting Event Configuration



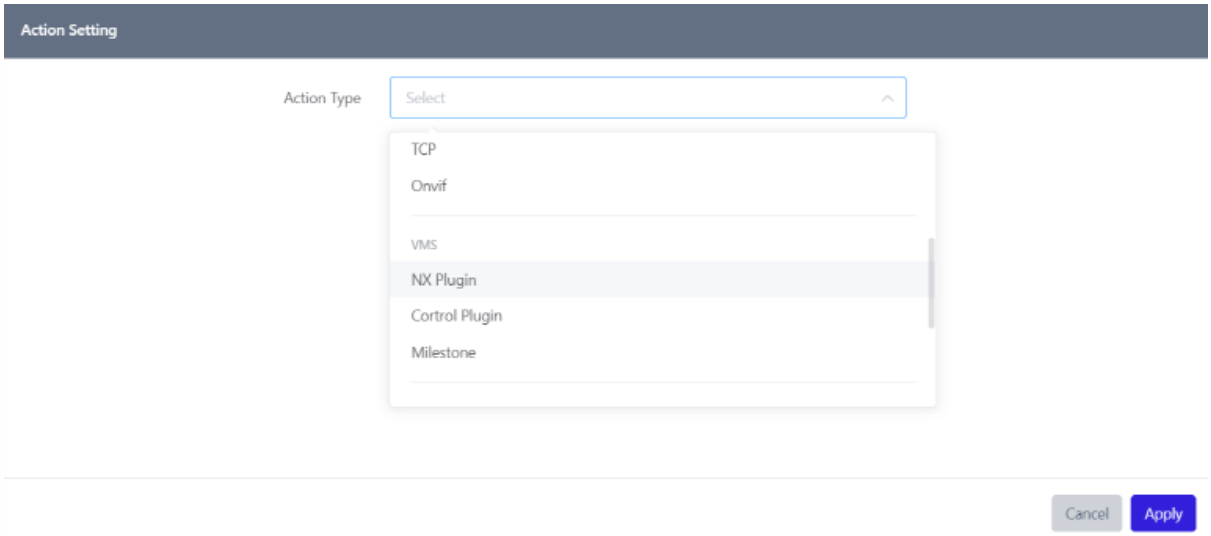
AIBOX's Event Name field is displayed as Caption field in NX VMS. It is recommended to enter a name that can identify the event. It is tagged to the object as shown in the figure below. Also, when registering a rule, you can set a detailed rule through text comparison in the caption field.



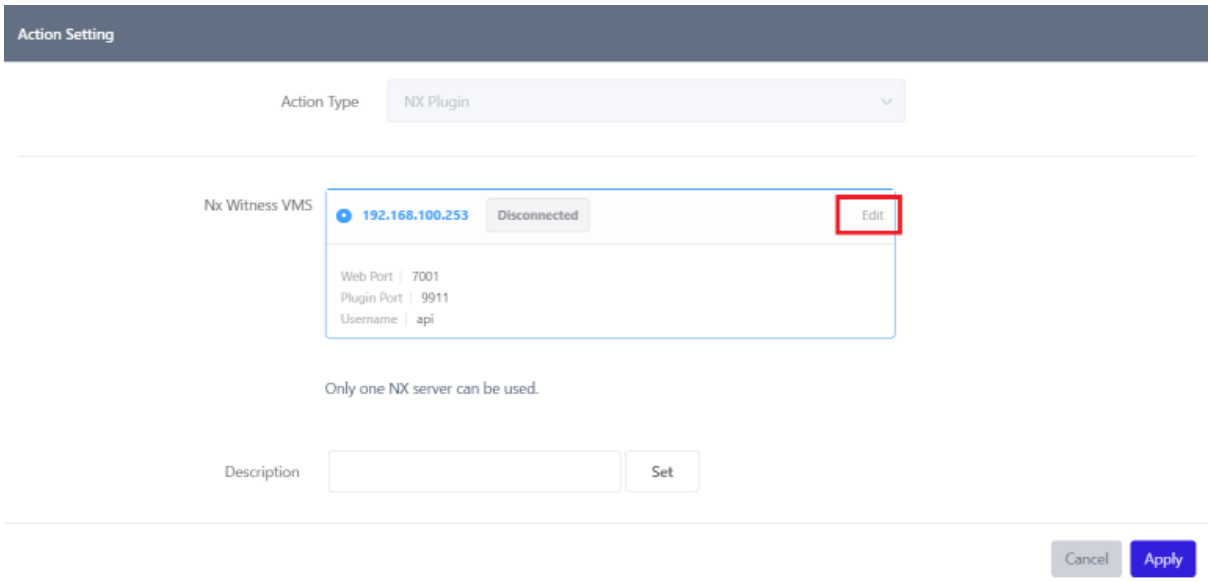
3.3 Adding NX Plugin action handler

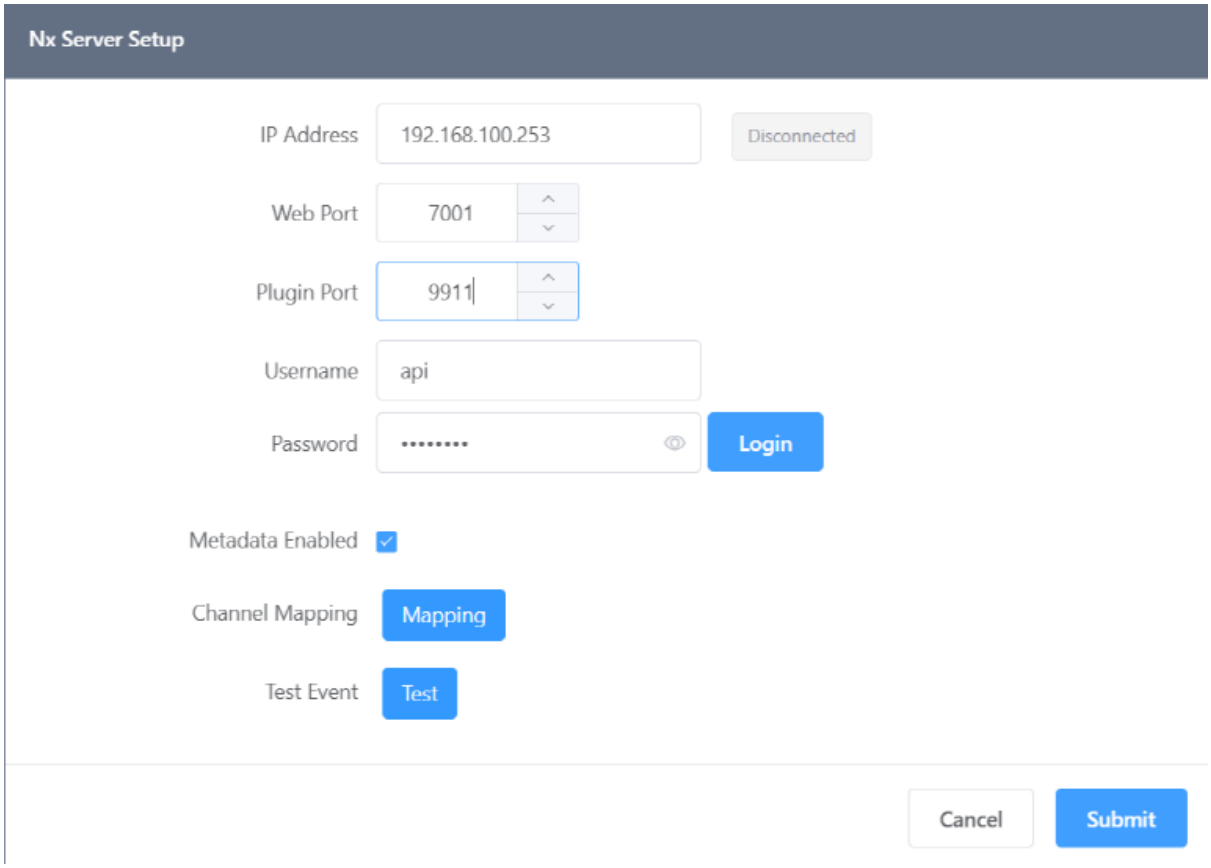
Add Action Setting

Select VMS / Nx Plugin



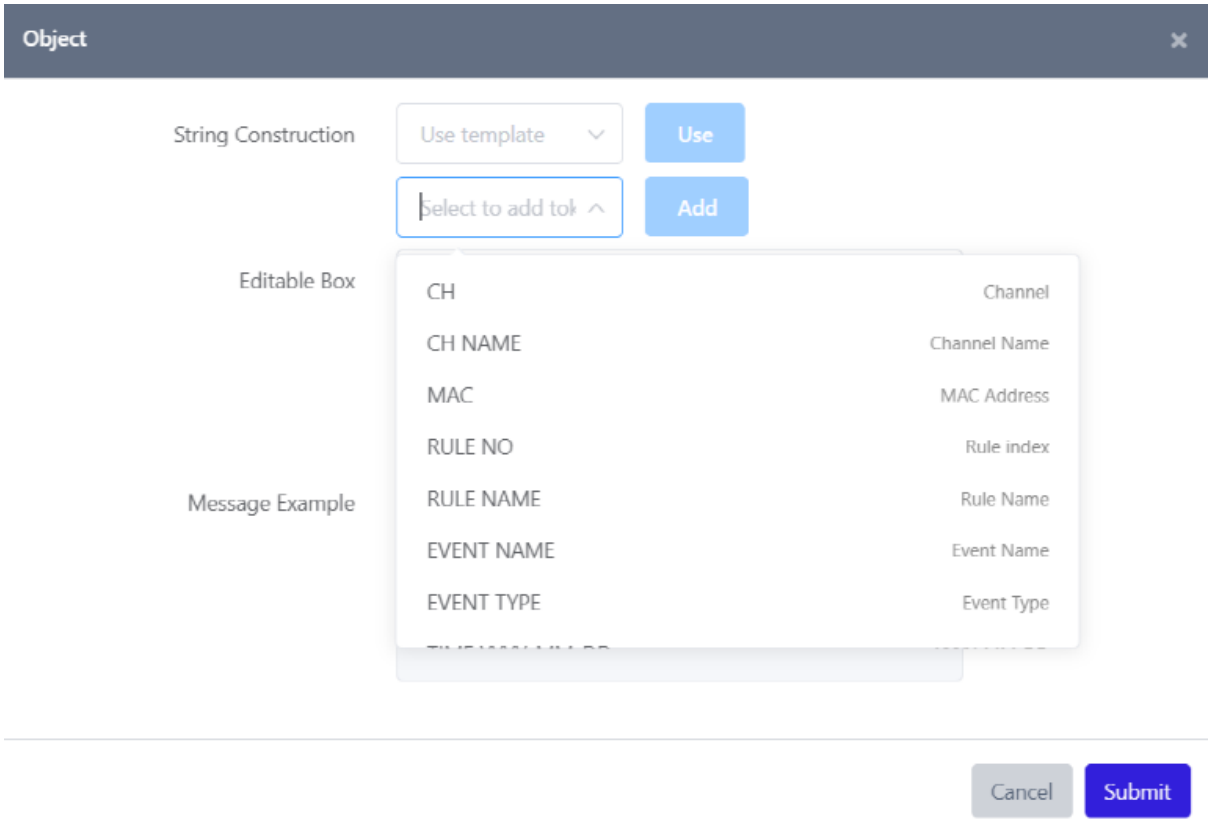
Editing VMS IP and Account





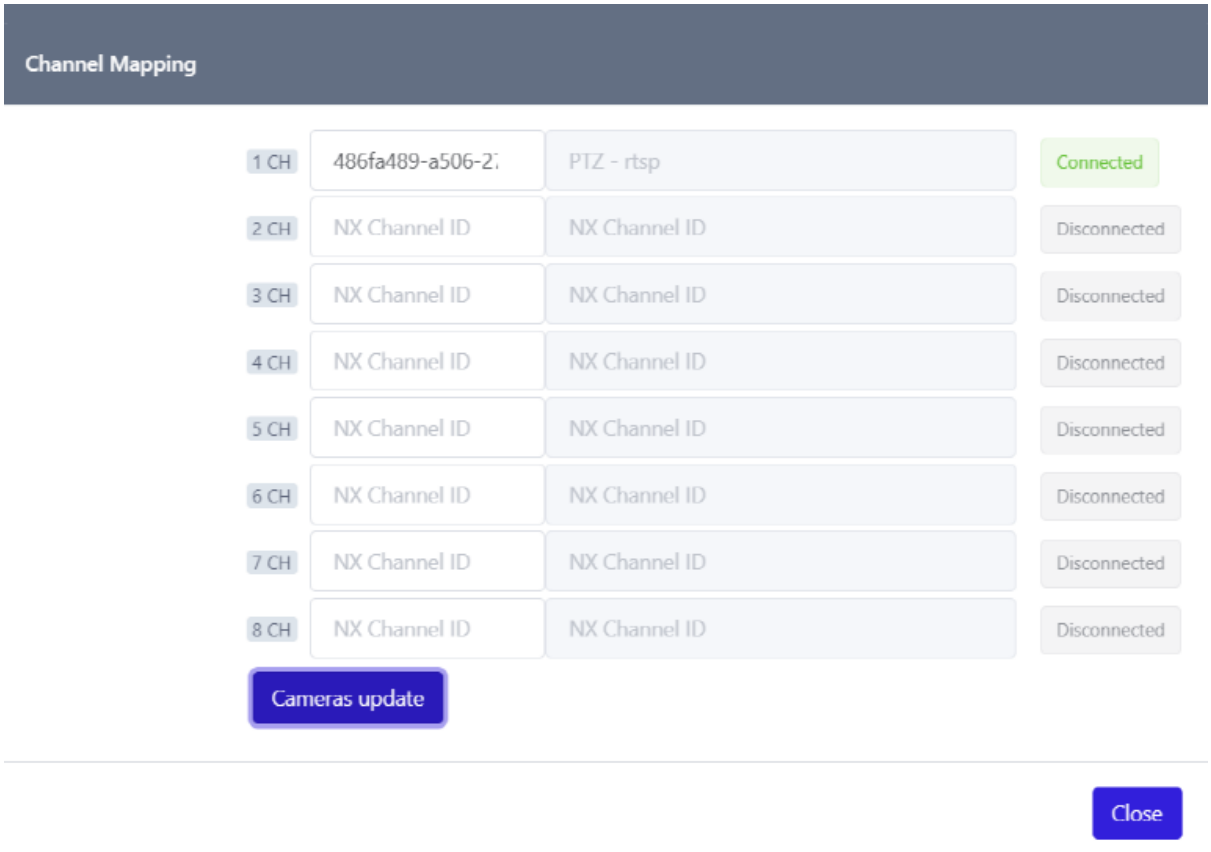
Enter the **“api” (case sensitive) account information** added in the previous step and **test using the Login button**. If the test is successful, you will see a connected green status indicator.

Additional object information can be passed to NX VMS through the Description field. (For example, LPR app license plate recognition information, group information)

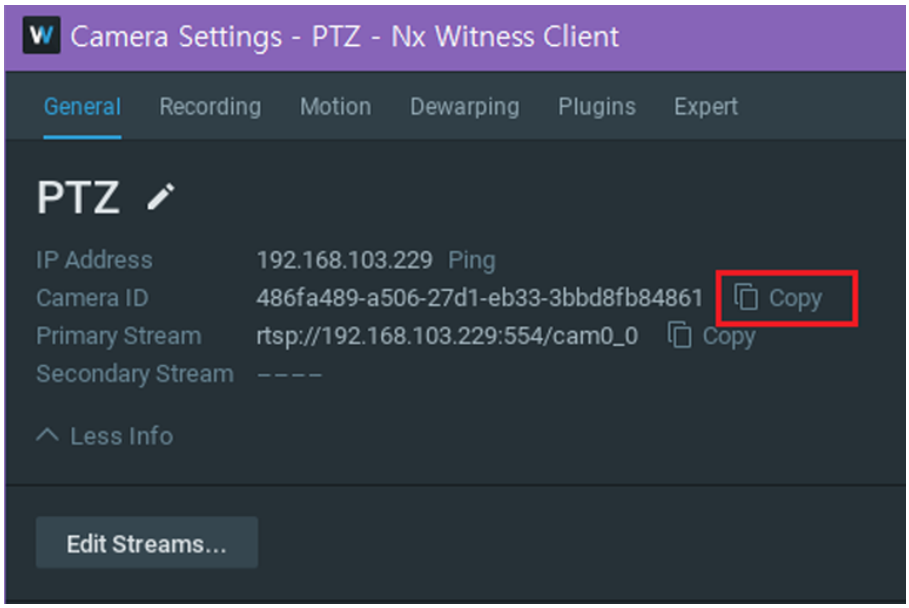


Channel Mapping

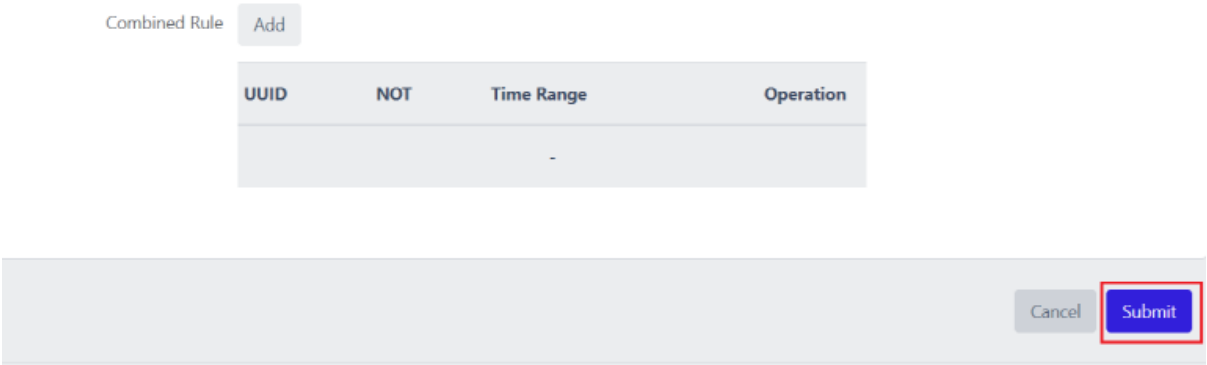
Channel information connection between AIBOX and NX VMS is required. If the channel id is entered correctly, the green Connected status will be displayed when you click the Camera Update button.



NX channel ID (Camera ID) information can be copied from the camera setup menu of NX VMS.



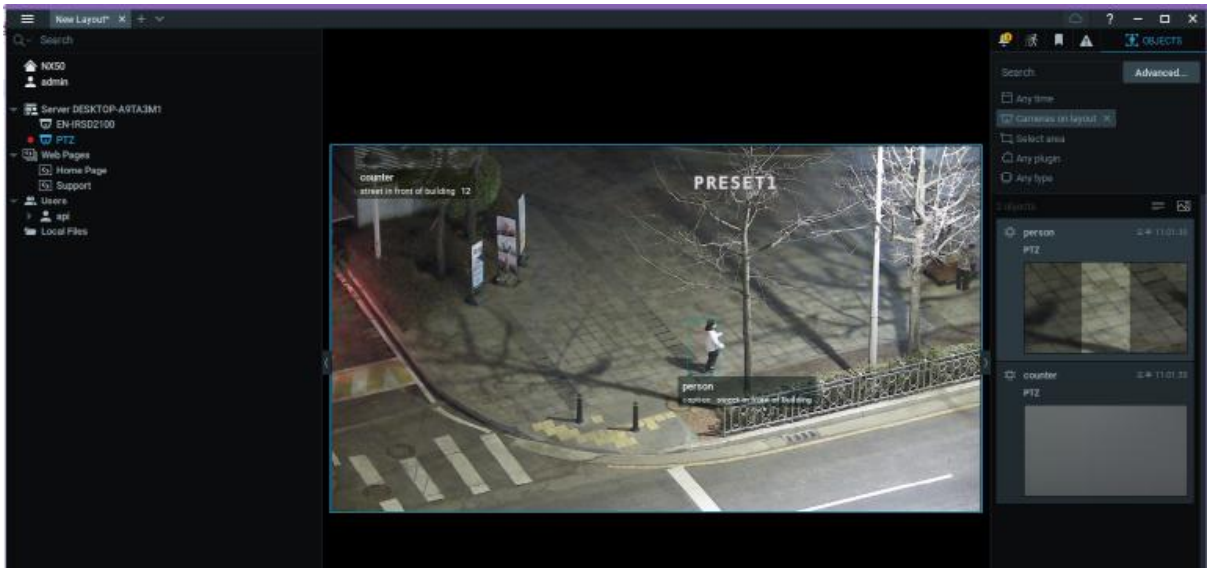
After completing all settings, click the Submit button at the bottom of the webpage. Your settings will not be saved unless you click the submit button.



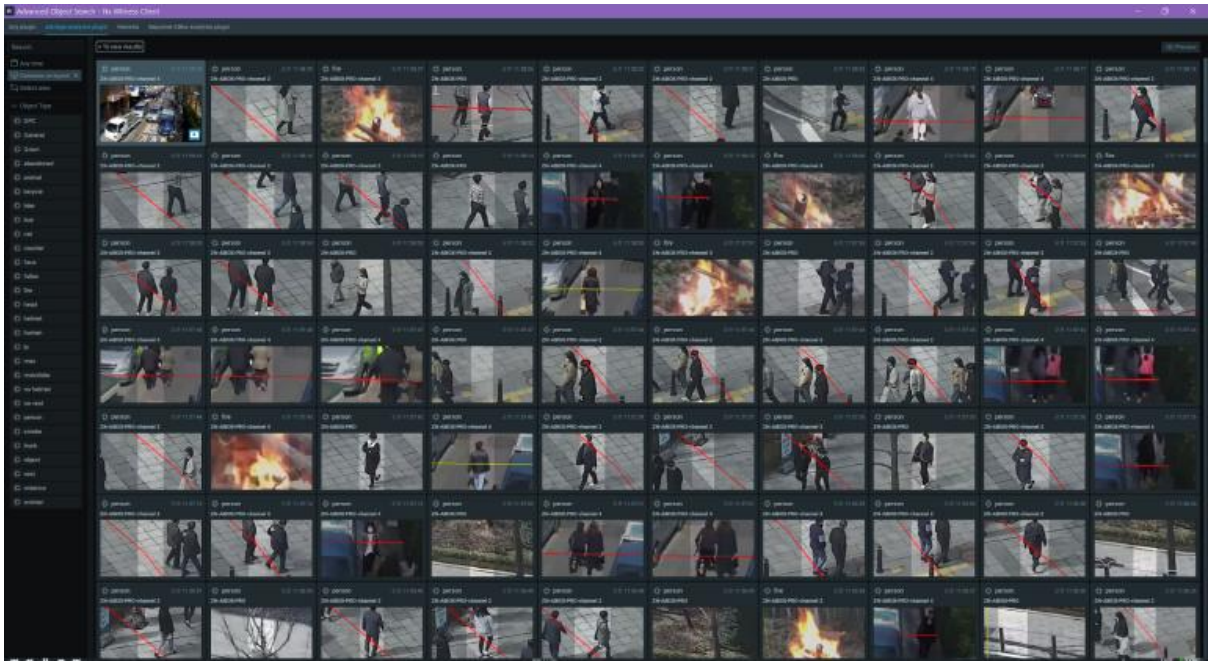
4. Demo

4.1 Live

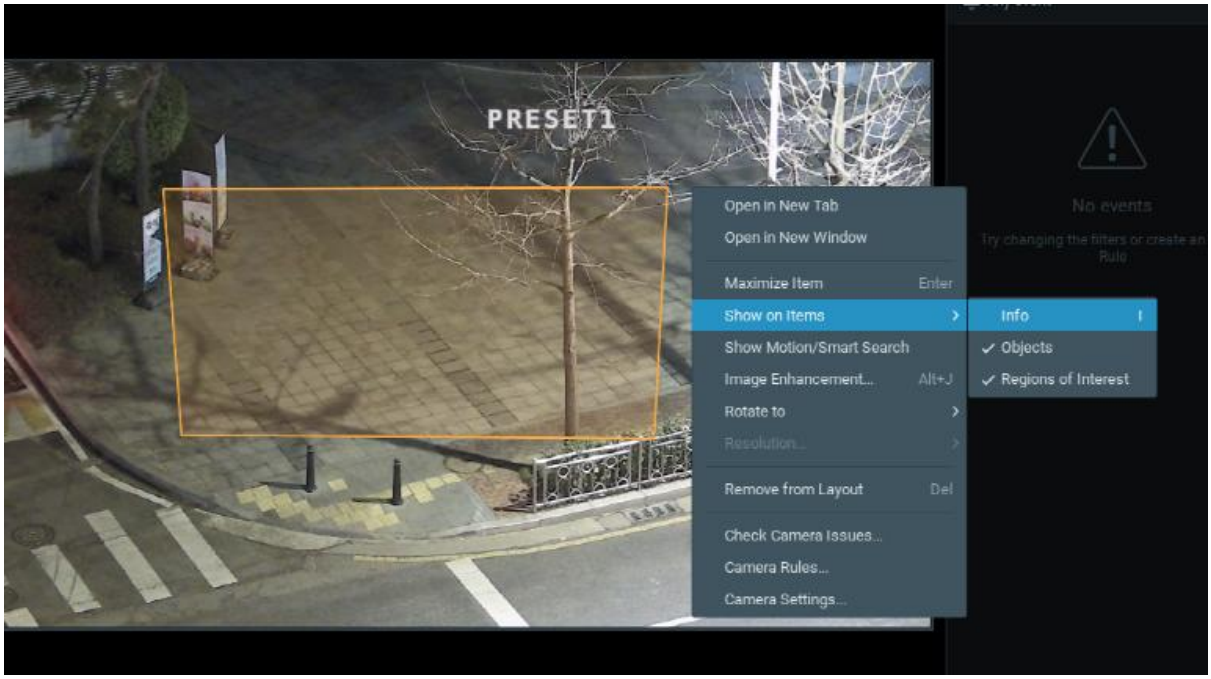
Objects with loitering person events are displayed in the NX VMS OBJECTS panel.



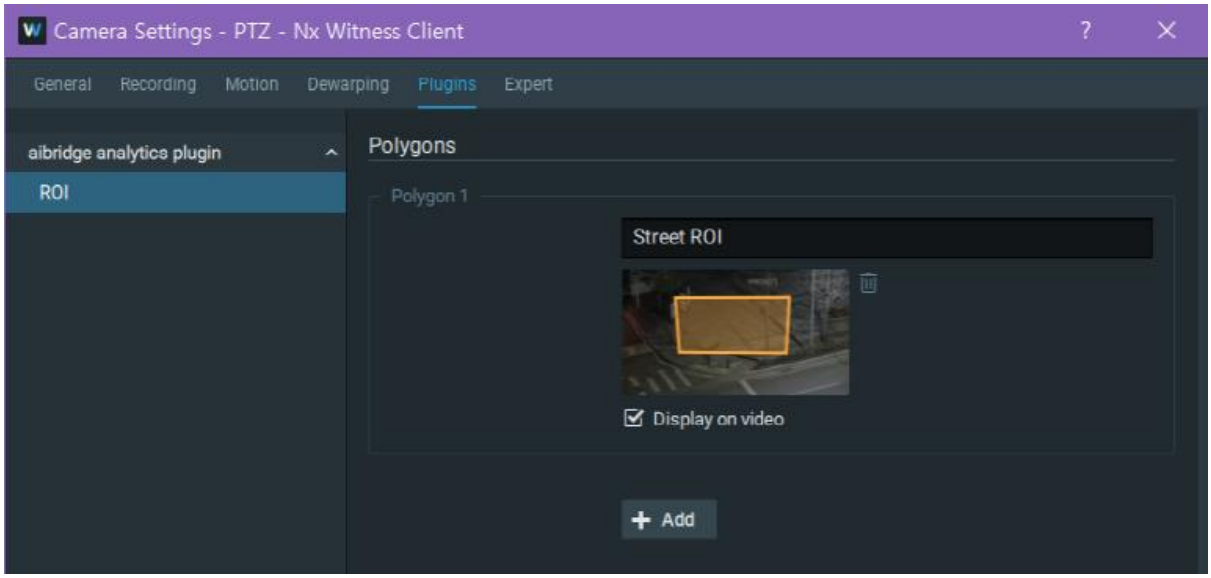
Saved objects can be searched through the Object “Advanced” menu of NX VMS.



When objects are not visible, activate Objects in “Show on Items” in the popup menu of the video window.



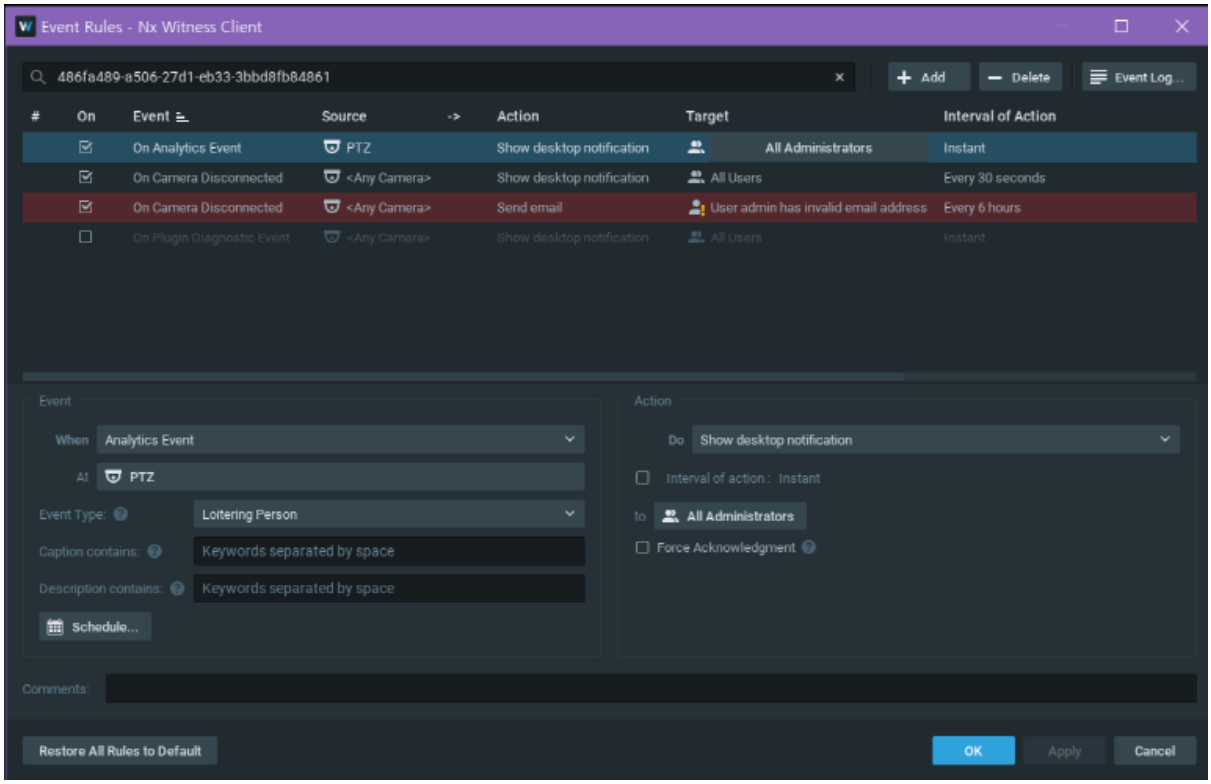
You can then manually specify the ROI area. It is automatically synchronized with the ROI(zone) information of AIBOX through AIBOX F/W upgrade in the future.



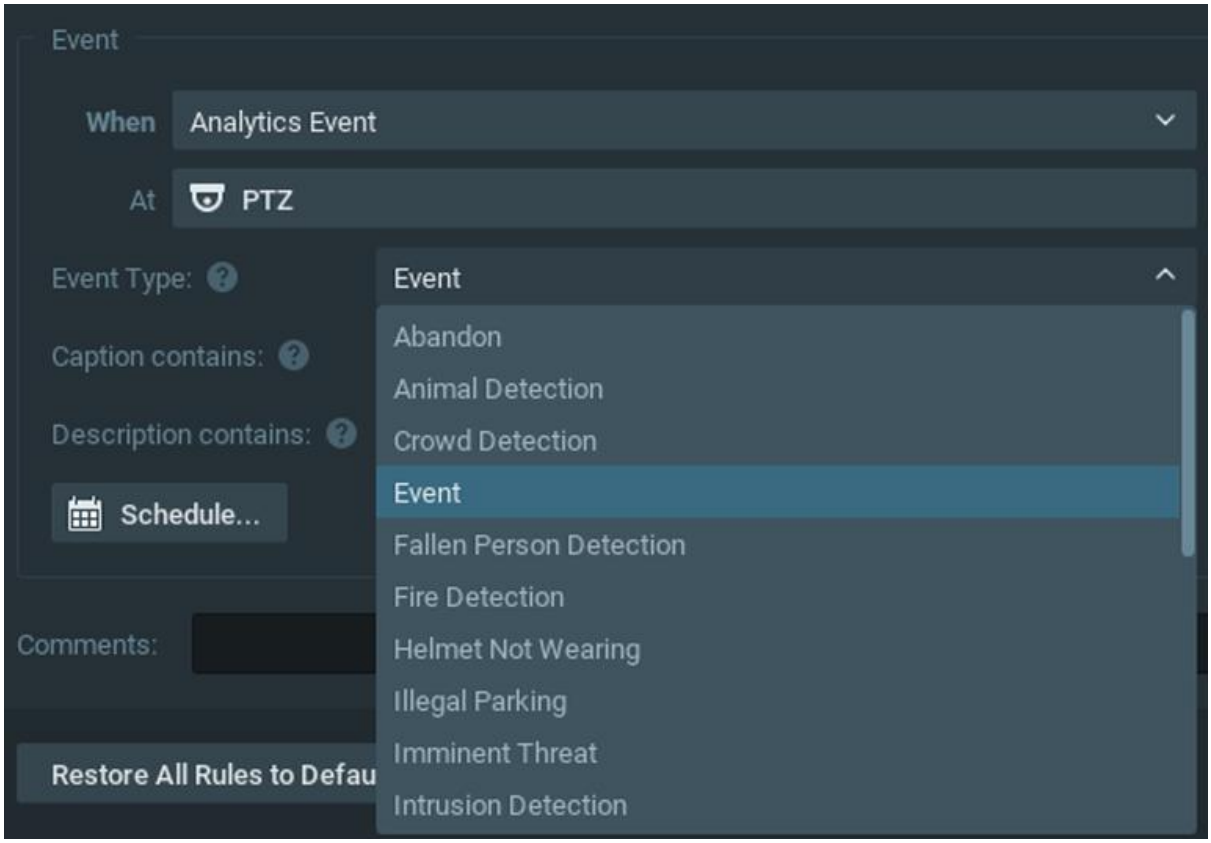
4.2 Add Nx VMS Event Rules

If you set the desktop notification action by adding Camera Rules in NX VMS, you can see the event in the NX VMS EVENTS panel.

When registering camera rules, pay attention to the “Event Type” setting. If the APP set in AIBOX and the Event Type do not match, the event will not occur.



note) If the AIBOX Analytics plugin is not up-to-date, there may be no App Event Type supported by AIBOX FW. In that case, select “Event” as the Event Type.

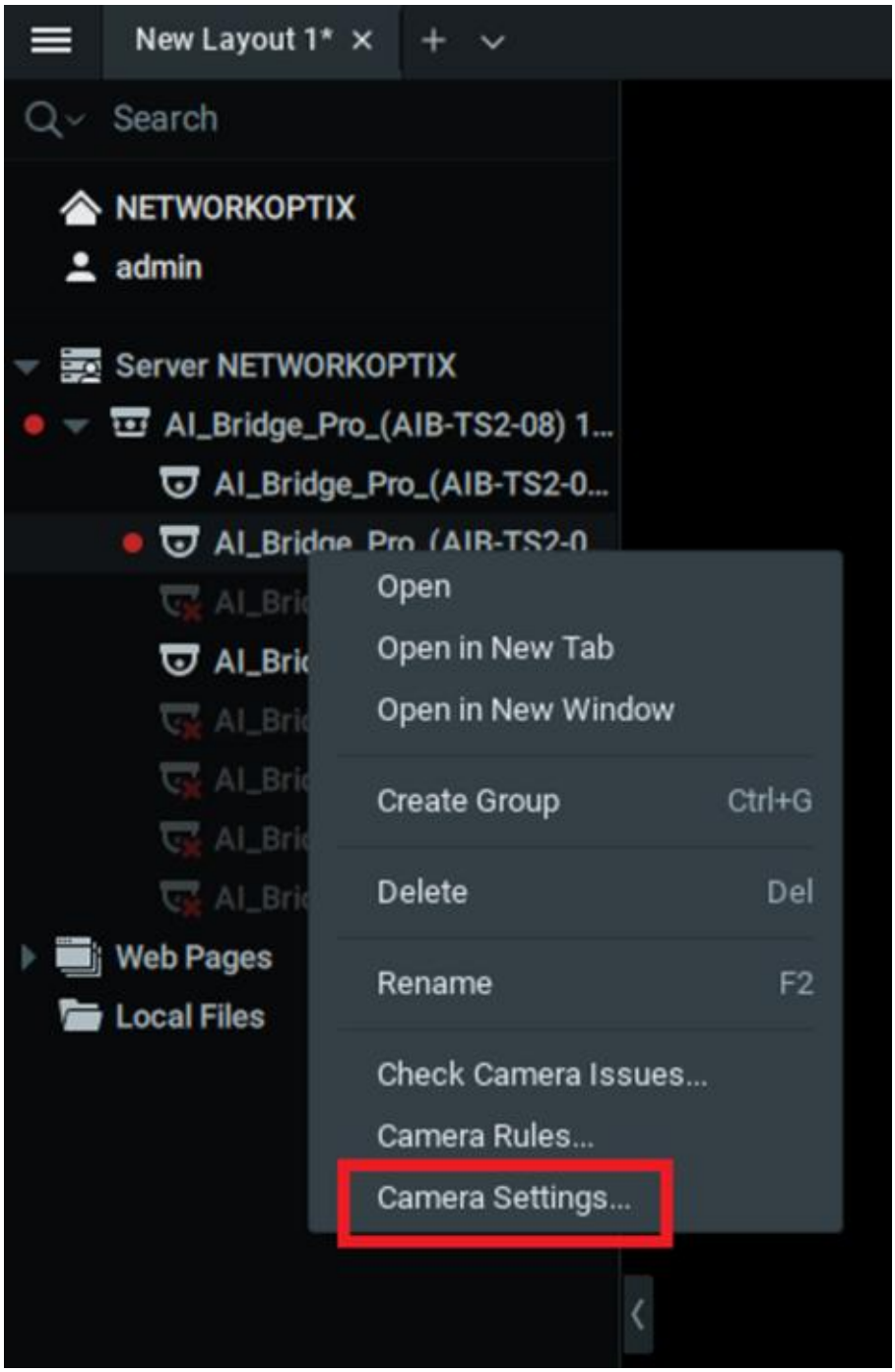


5. FAQ

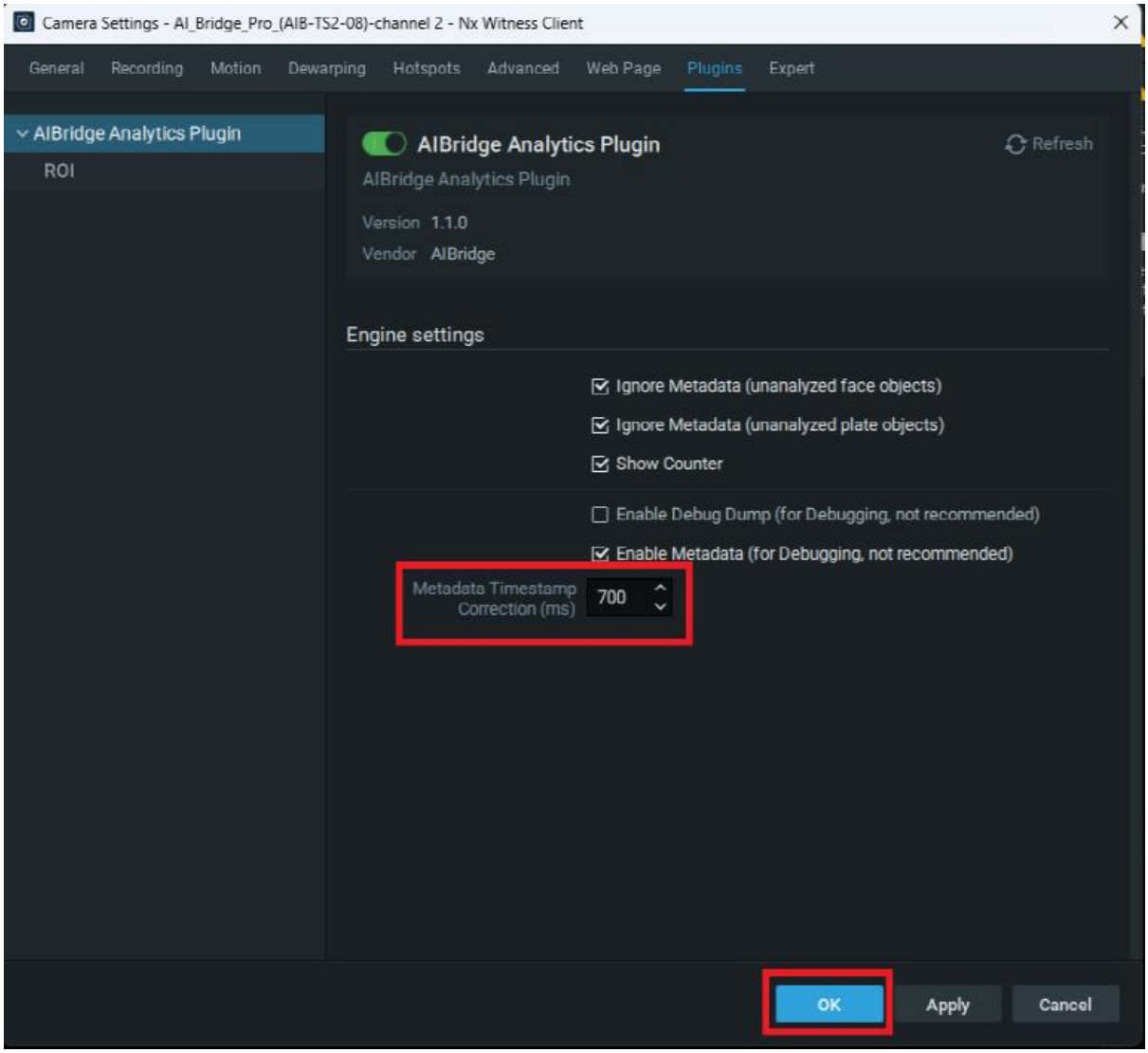
5.1 Solution for Video Delay

This session explains how to adjust the timestamp when the bounding box in Network Optix does not match the object (when a delay occurs).

Right-click on the camera and then click “Camera Settings.”



Set the Metadata Timestamp to an appropriate value and click the “OK” button. (Typically, values between 500 and 1000 are recommended, but it may vary depending on the network environment.)



Immix Integration Guide

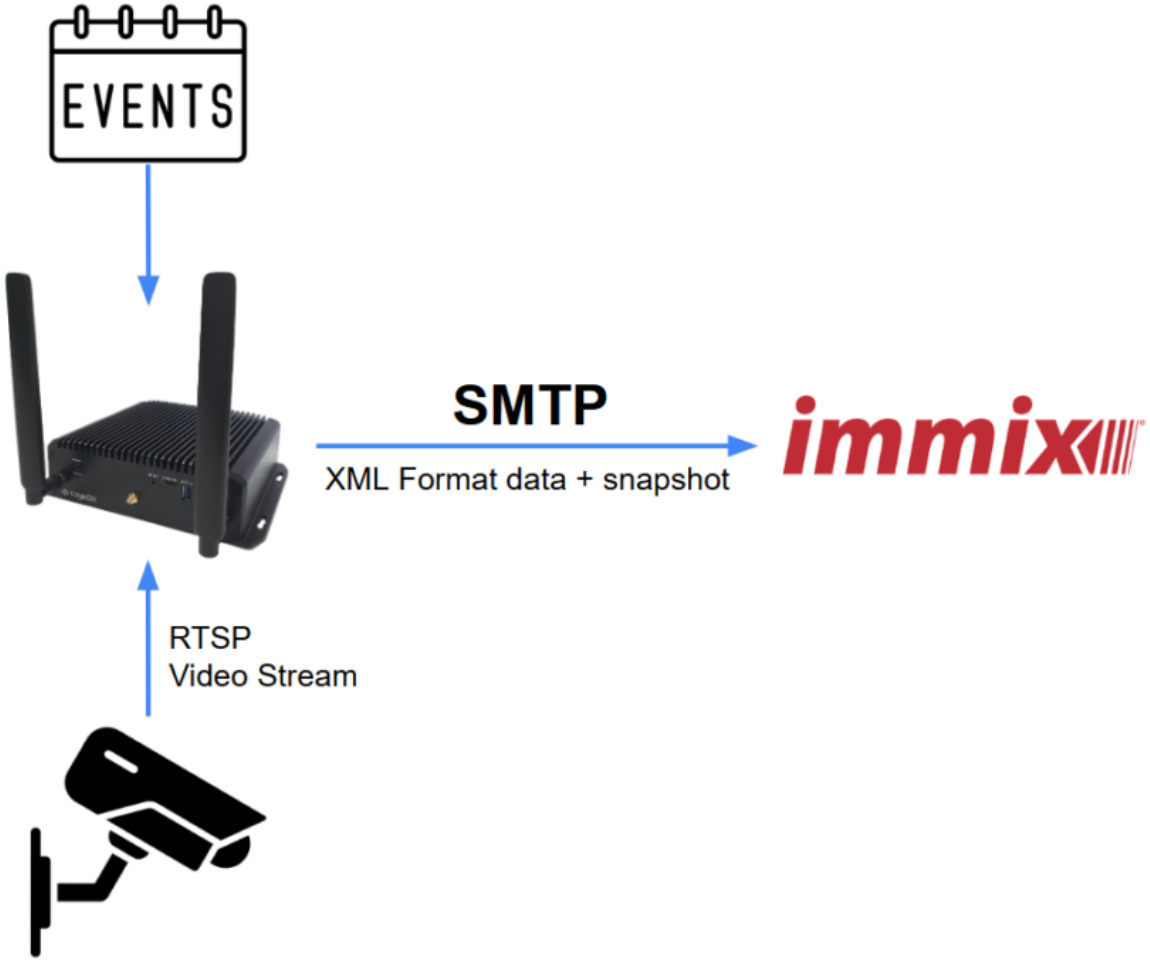
1. Introduction

1.1 Prerequisites

- AIBOX FW version 100127 or higher.

1.2 Learn about integration architecture

In IMMIX integration, event messages are sent using SMTP. Video is received through RTSP Stream, and when an event is triggered by setting up an AI Rule, the event message in XML format is sent along with the video from that time period.



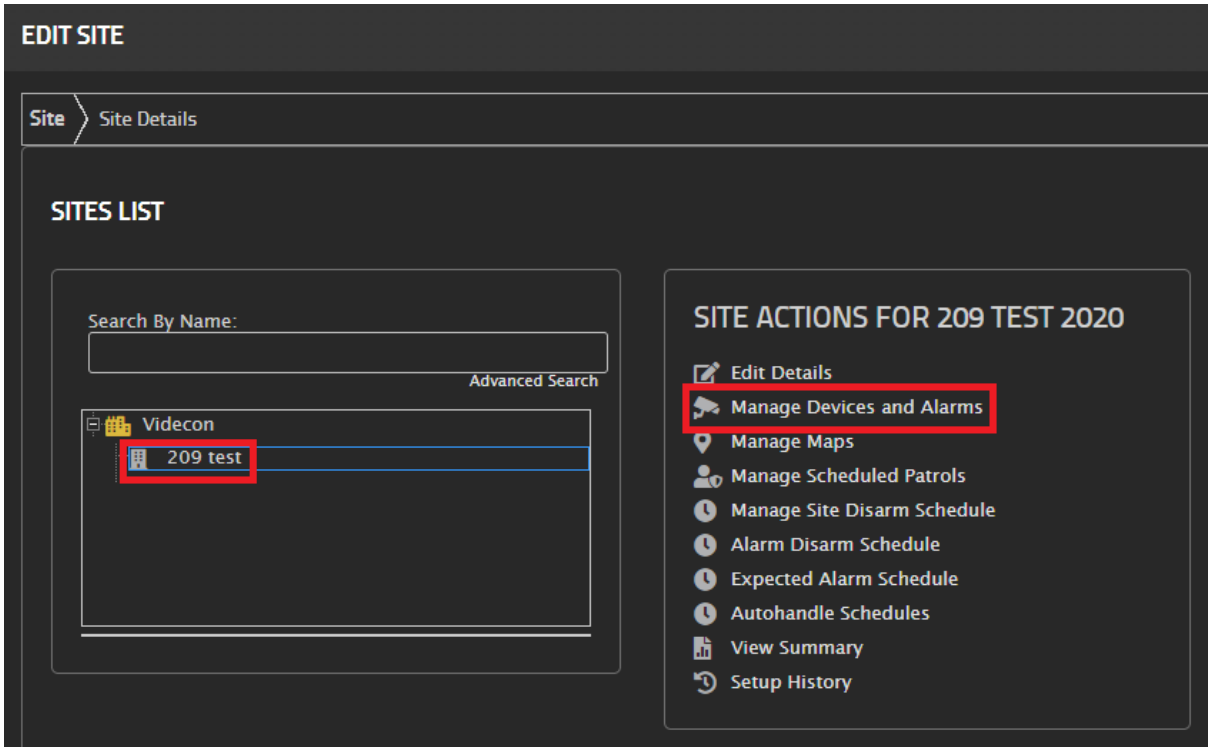
2. Configuration

To use Immix, some settings need to be configured. Please follow the steps below.

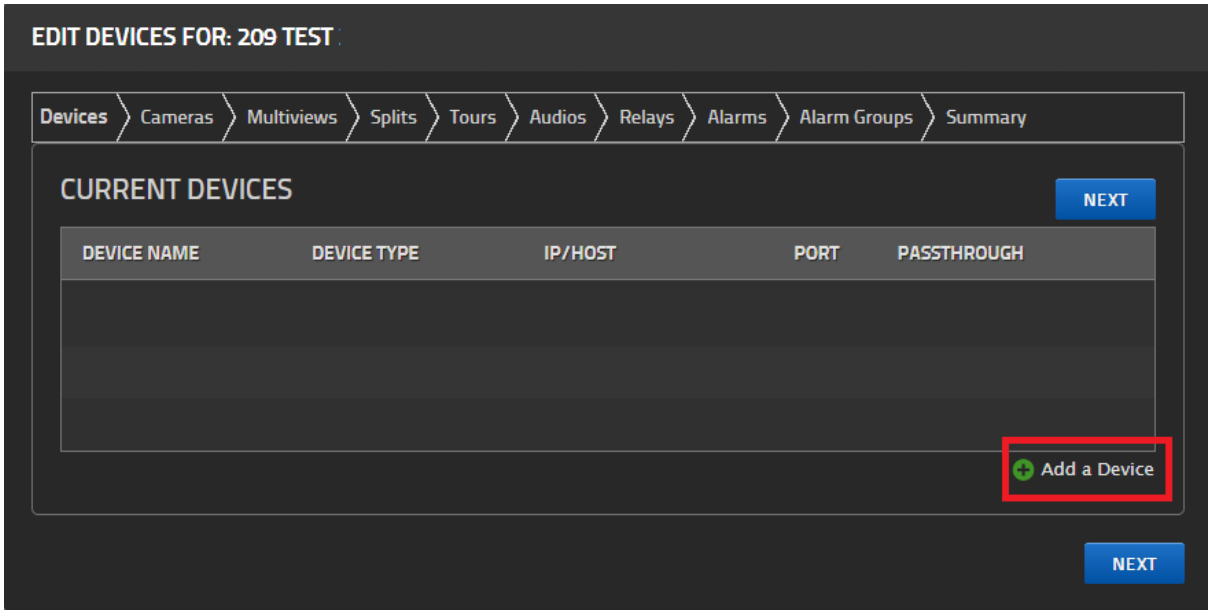
2.1 Immix Configuration

In order to link AIBOX and Immix, you must register AIBOX in Immix. Watch and follow below. First you need to add equipment.

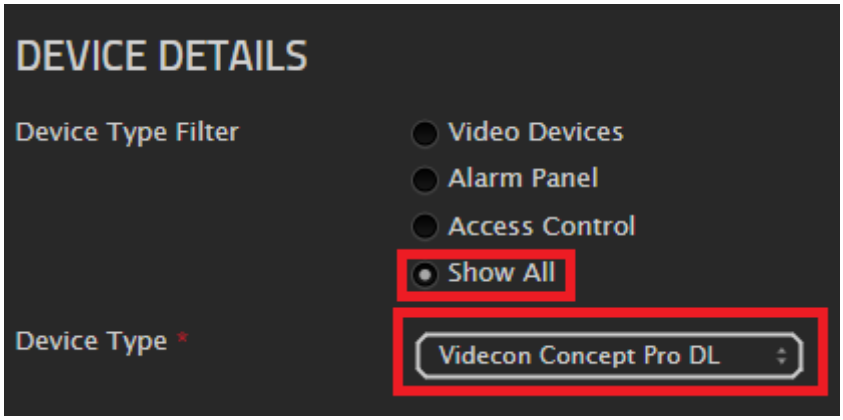
Click the site where you want to add the device, and then click Manage Devices and Alarms.



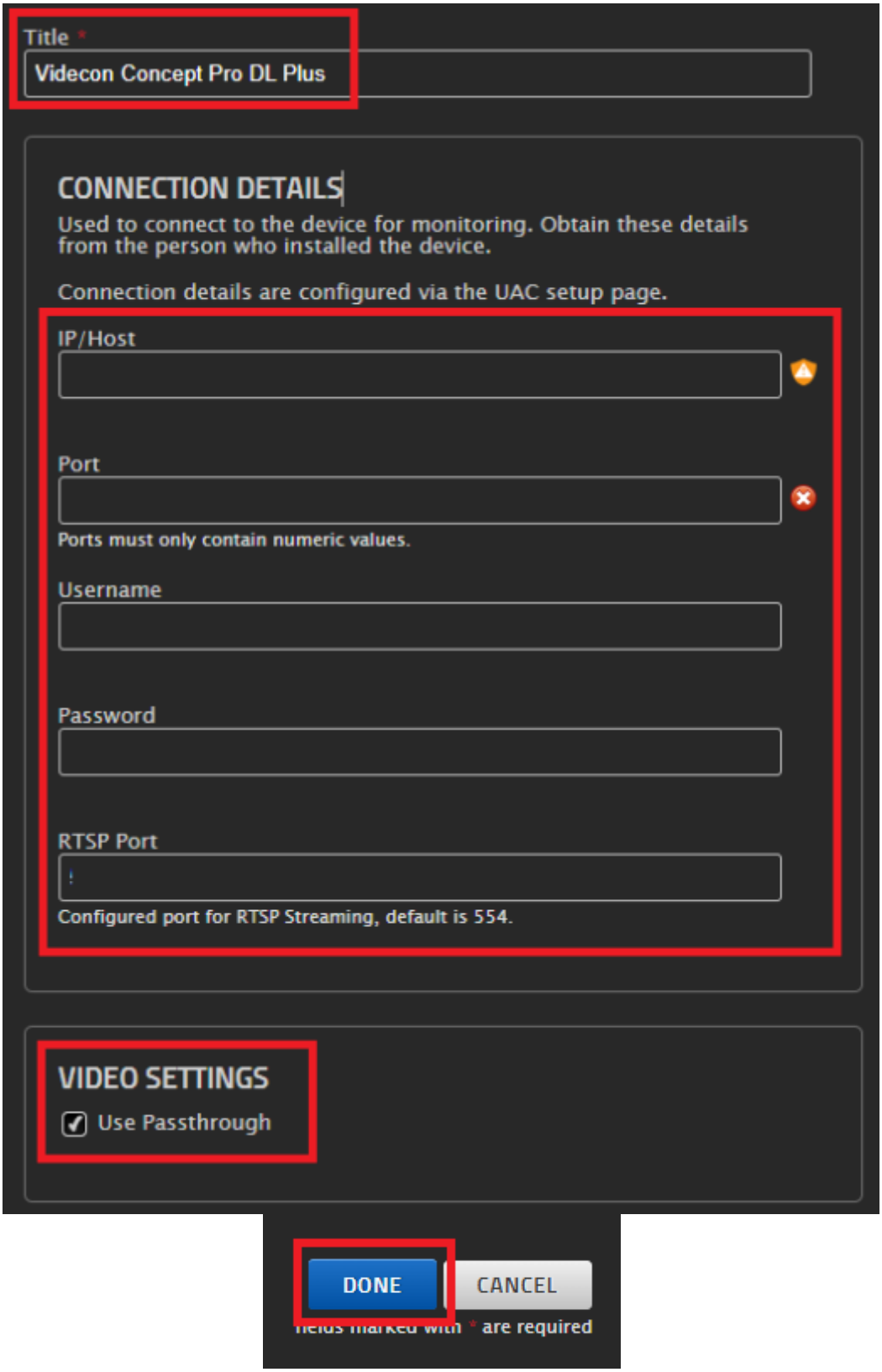
Click the “Add a Device”



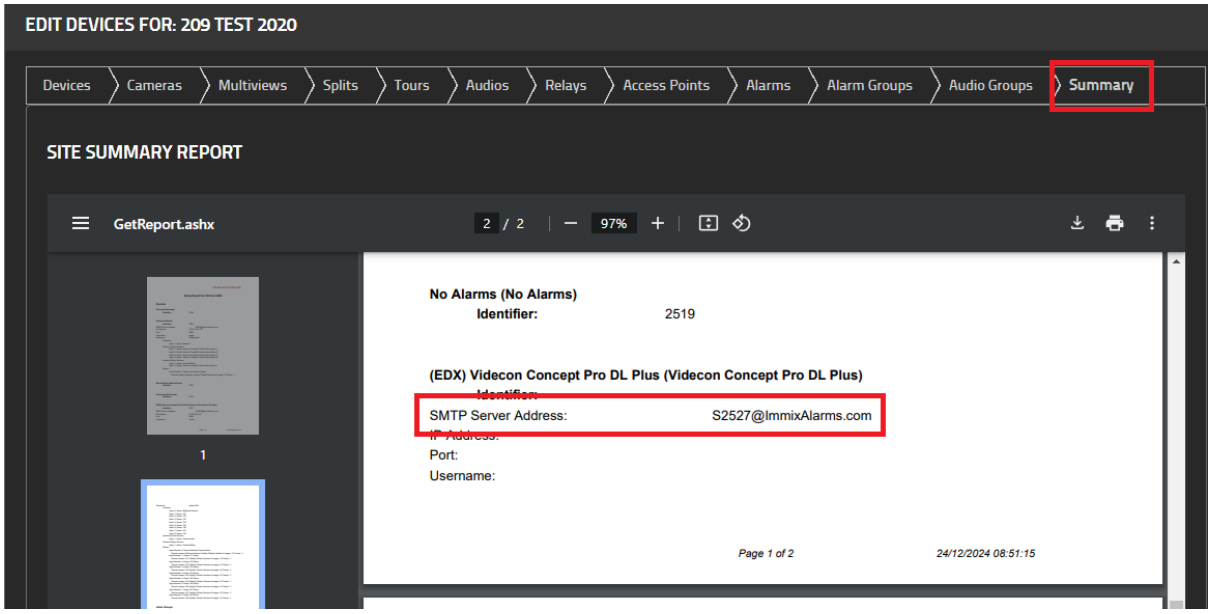
In the Device Type Filter, select “Show All” and choose “Videcon Concept Pro DL” for the Device Type.



Fill in the information for the device to be connected, check “Use Passthrough” under VIDEO SETTINGS, and then click the “DONE” button.



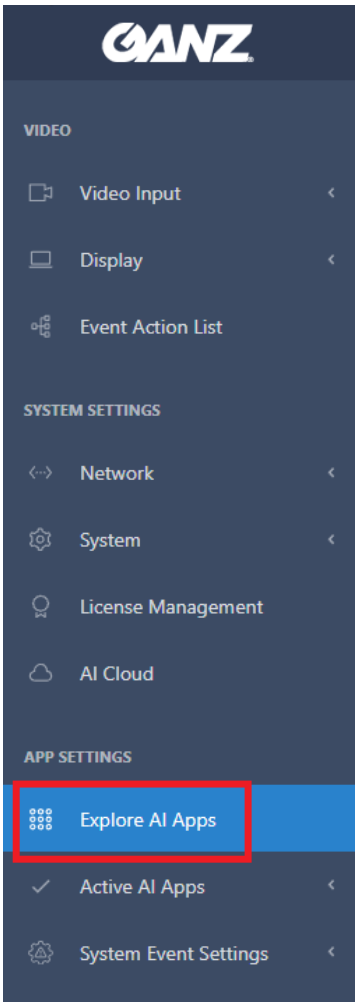
You can check the SMTP Server Address by going to “Summary” in the top menu.



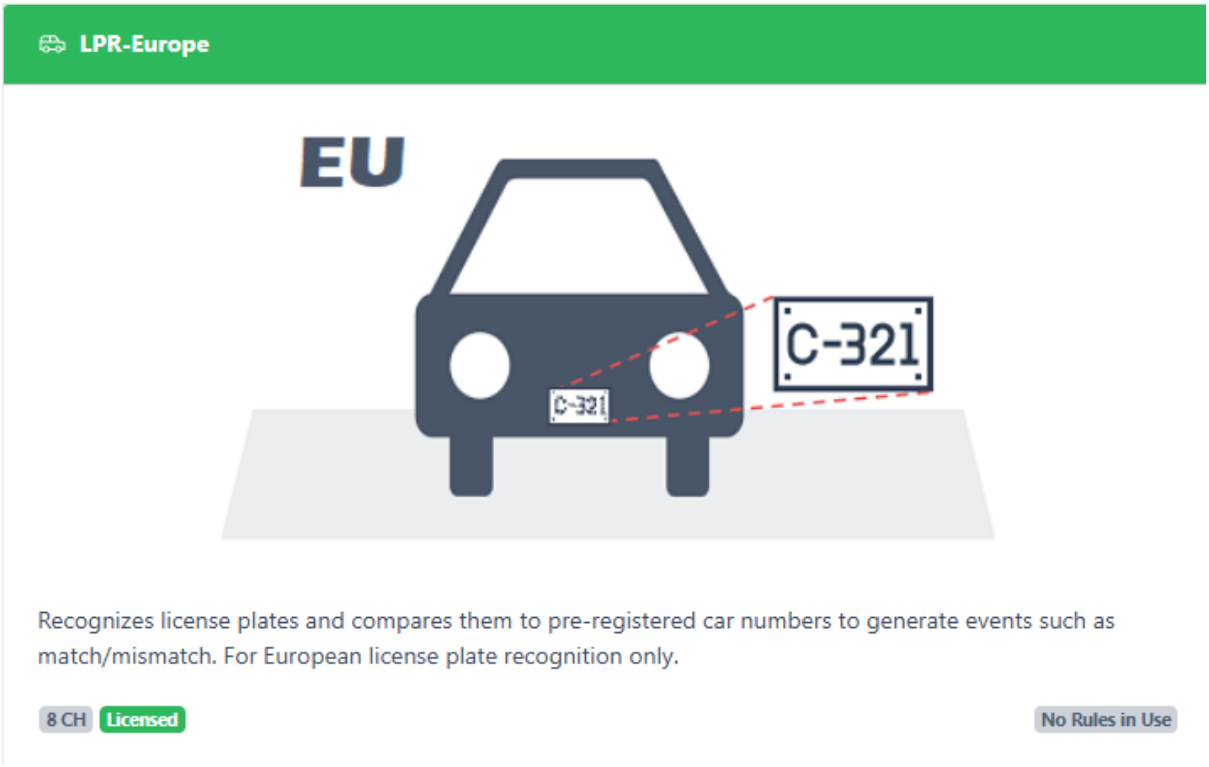
2.2 AIBOX Configuration

The method to use Immix integration in the AIBOX is as follows.

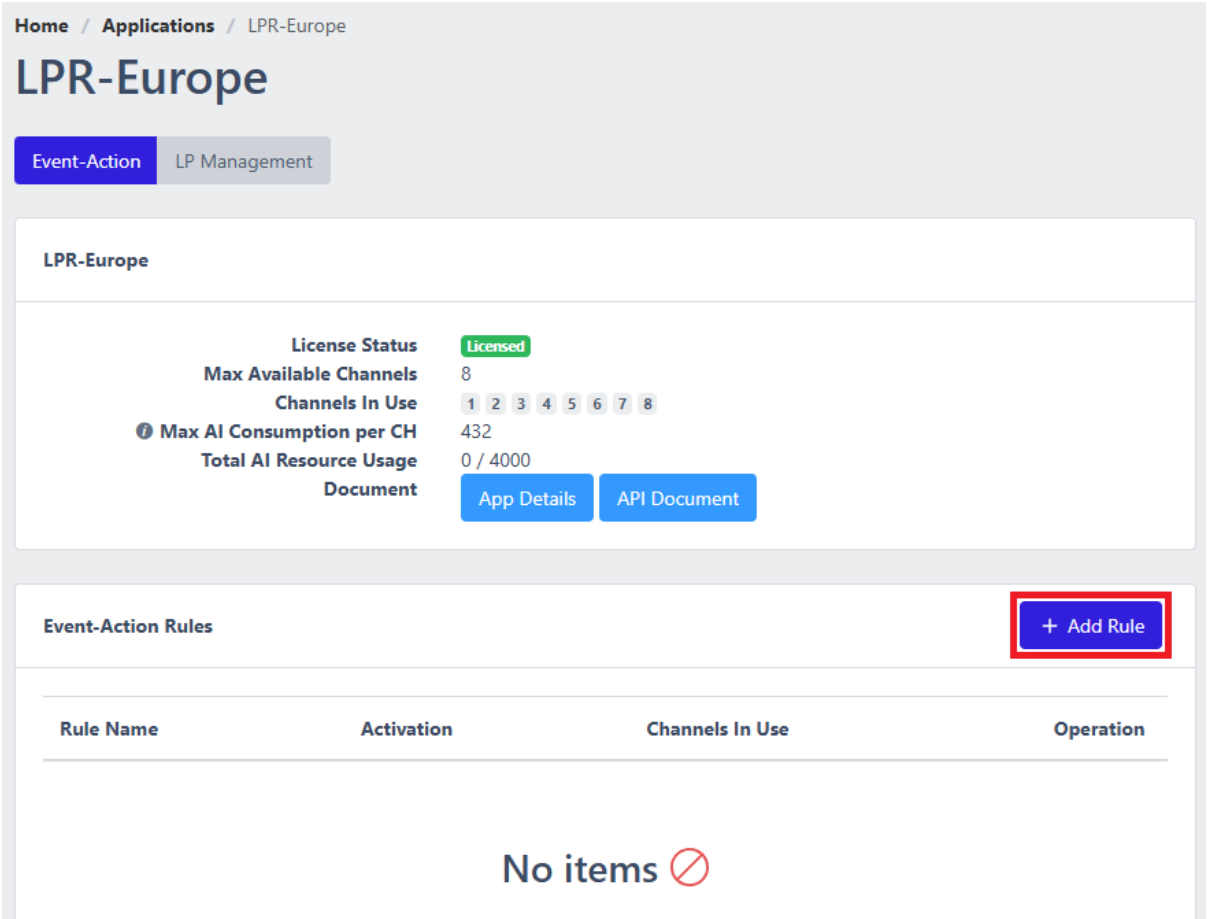
Access the AIBOX and click on “APP SETTINGS” > “Explore AI Apps” menu on the left sidebar.



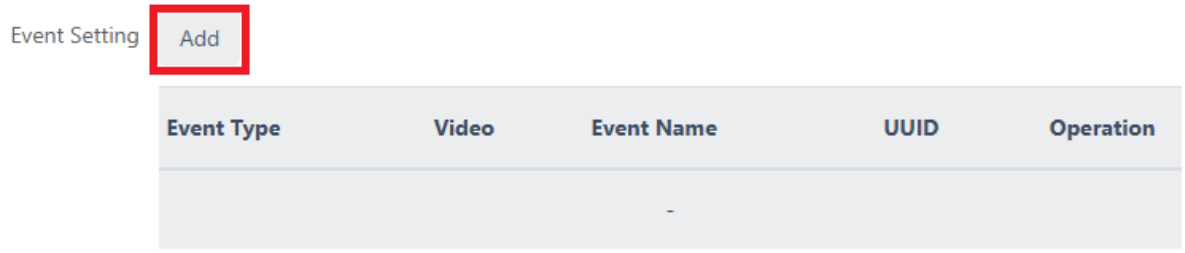
Please click on the event you want to use. In this manual, we will use LPR-Europe as an example.



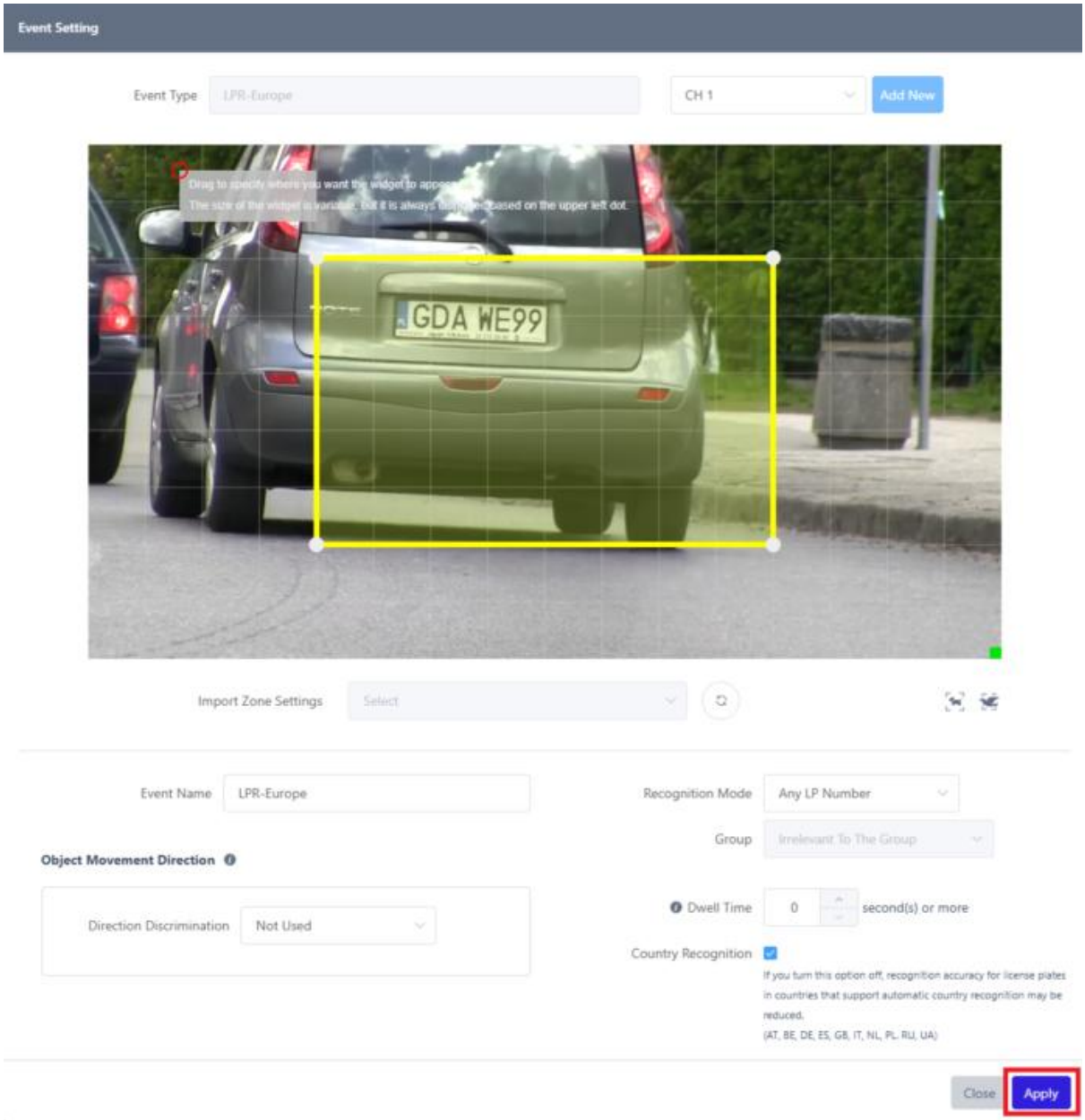
Please click the “Add Rule” button.



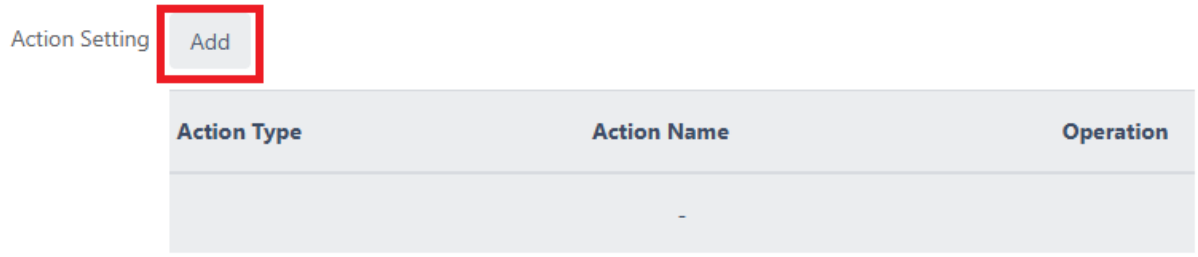
Click the “Add” button in the Event Setting.



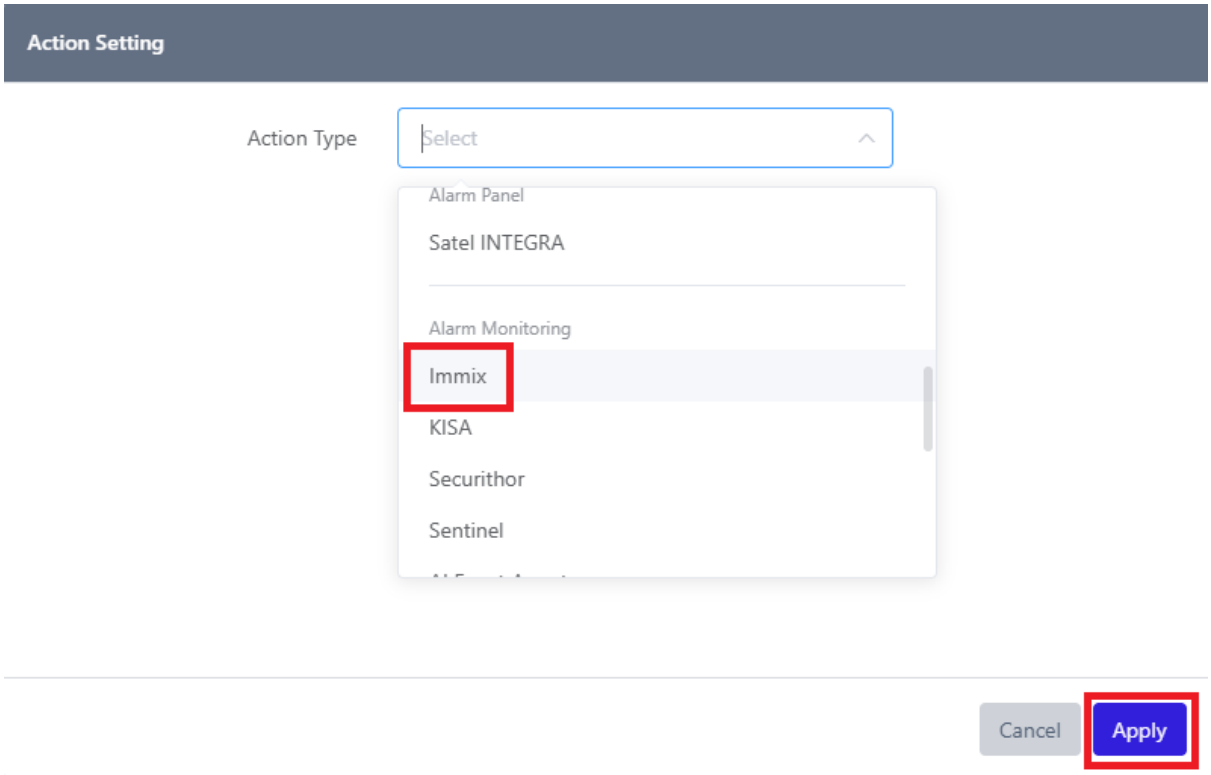
Zone or detailed setting of AI App. And Click the Apply button.



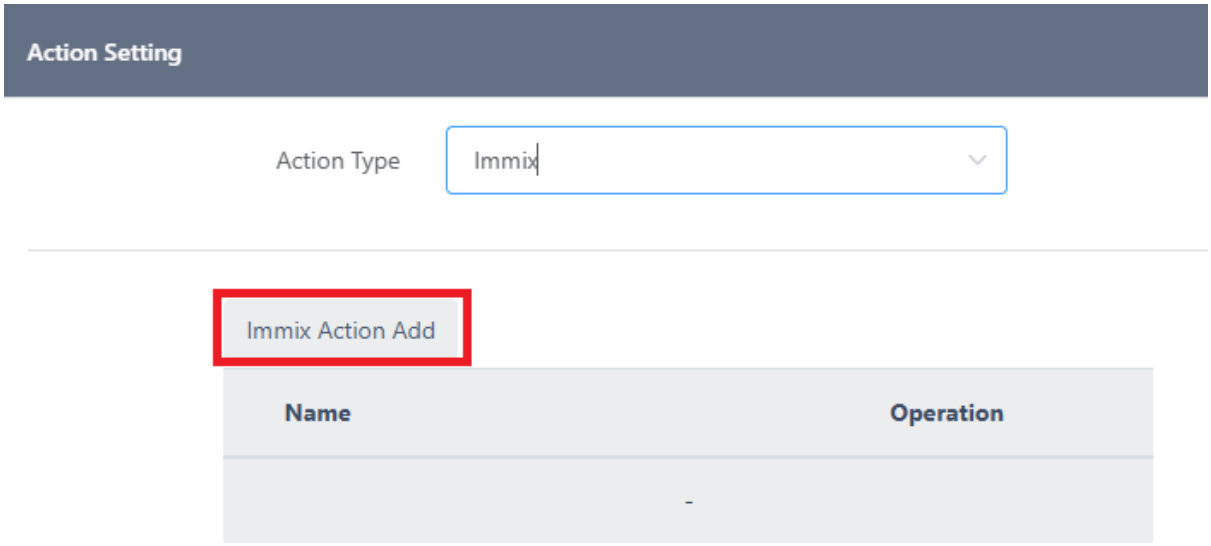
Click the “Add” button in the Action Setting.



Select “Immix” from the Action Type.



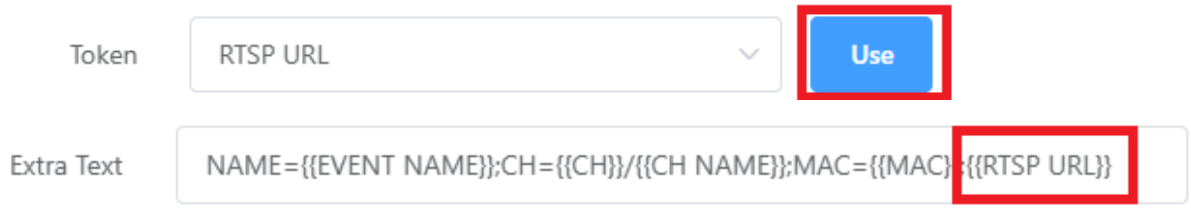
Click the “Immix Action Add” button.



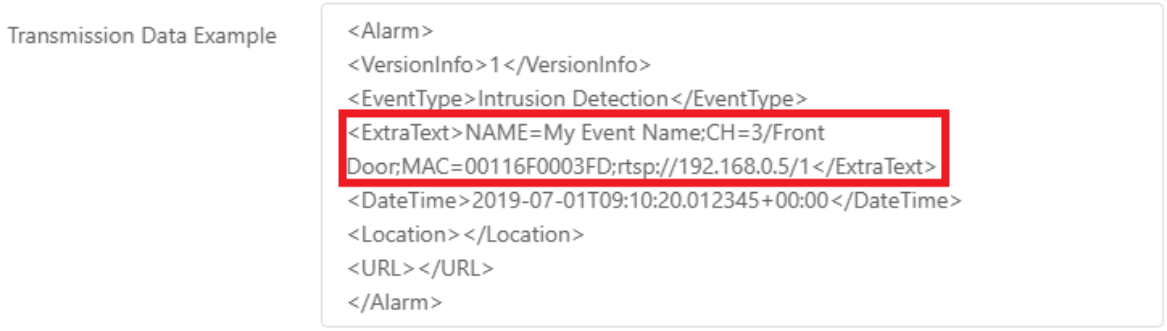
Enter the SMTP server and the account to receive the messages.

Enter “ukdemo.immixcs.net” for the SMTP server and use port 25. The recipient can be found in IMMIX. For more details, please refer to section 2.1.

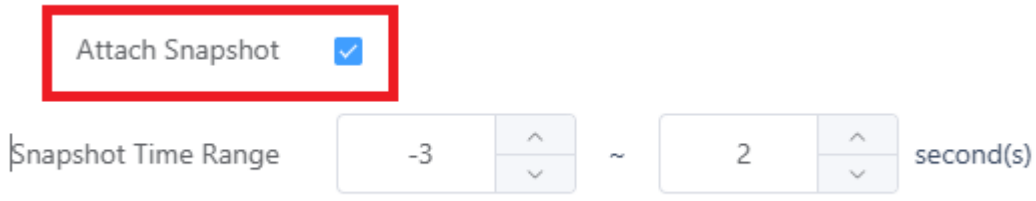
Click the desired token and press the “Use” button to add it to the Extra Text.



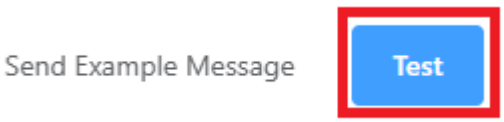
Only the Extra Text can be adjusted by the user in the transmitted data. Other fields, such as CH or Event Type, are automatically transmitted according to the corresponding event.



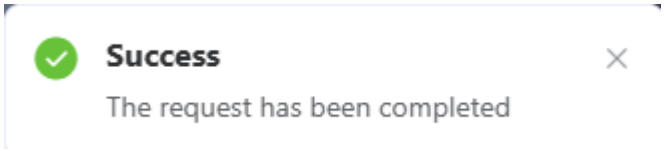
If you want to send a video along with the event, check “Attach Snapshot” and set the Time Range. The time is based on the event time (0 seconds); any time before is negative, and any time after is positive.



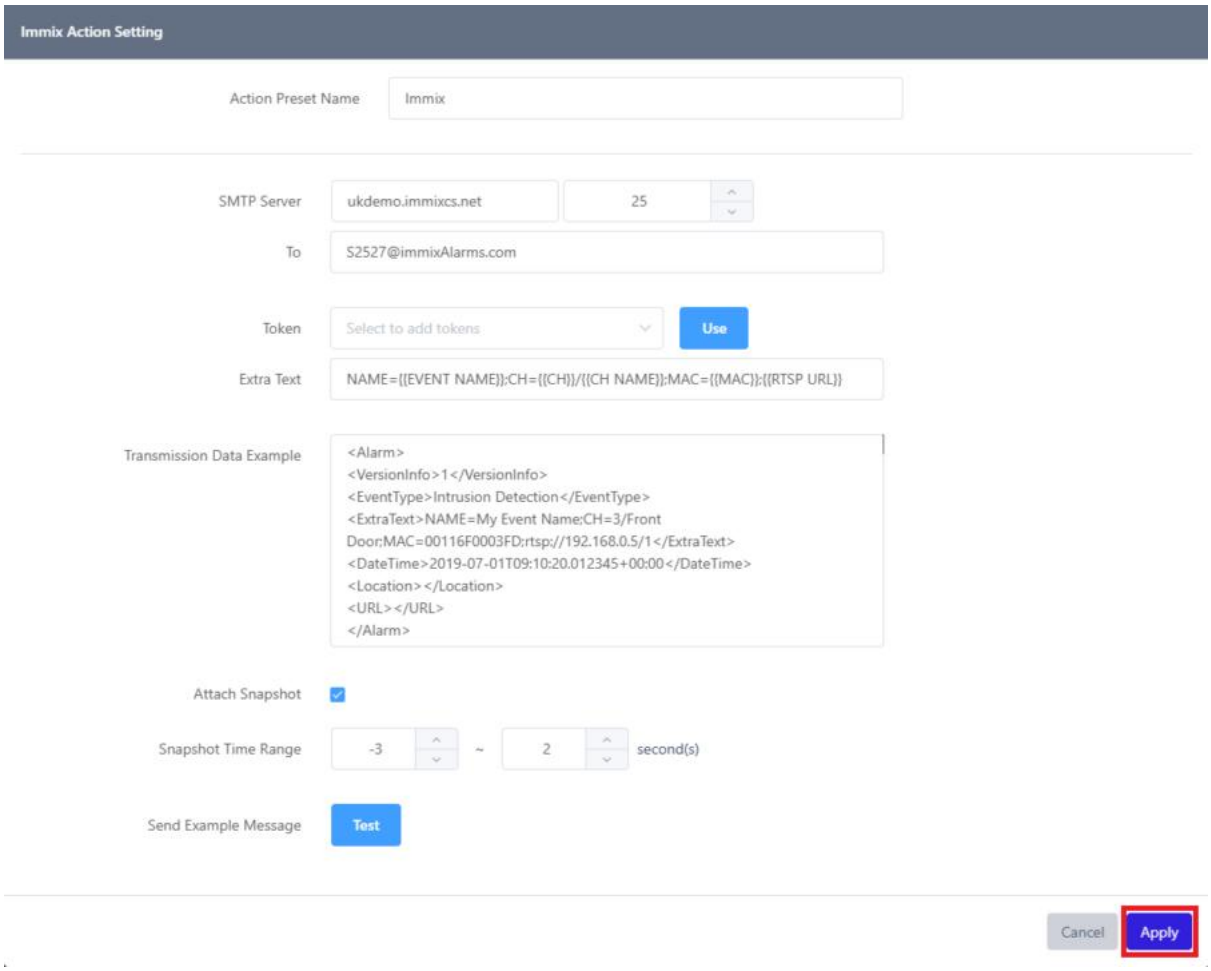
You can click the “Test” button to perform a test.



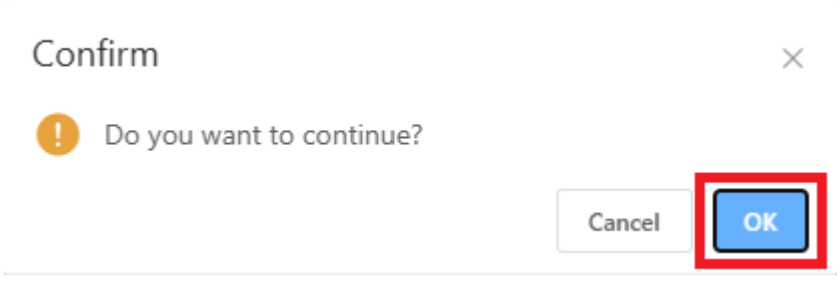
If the test is successful, a pop-up like the one below will appear.



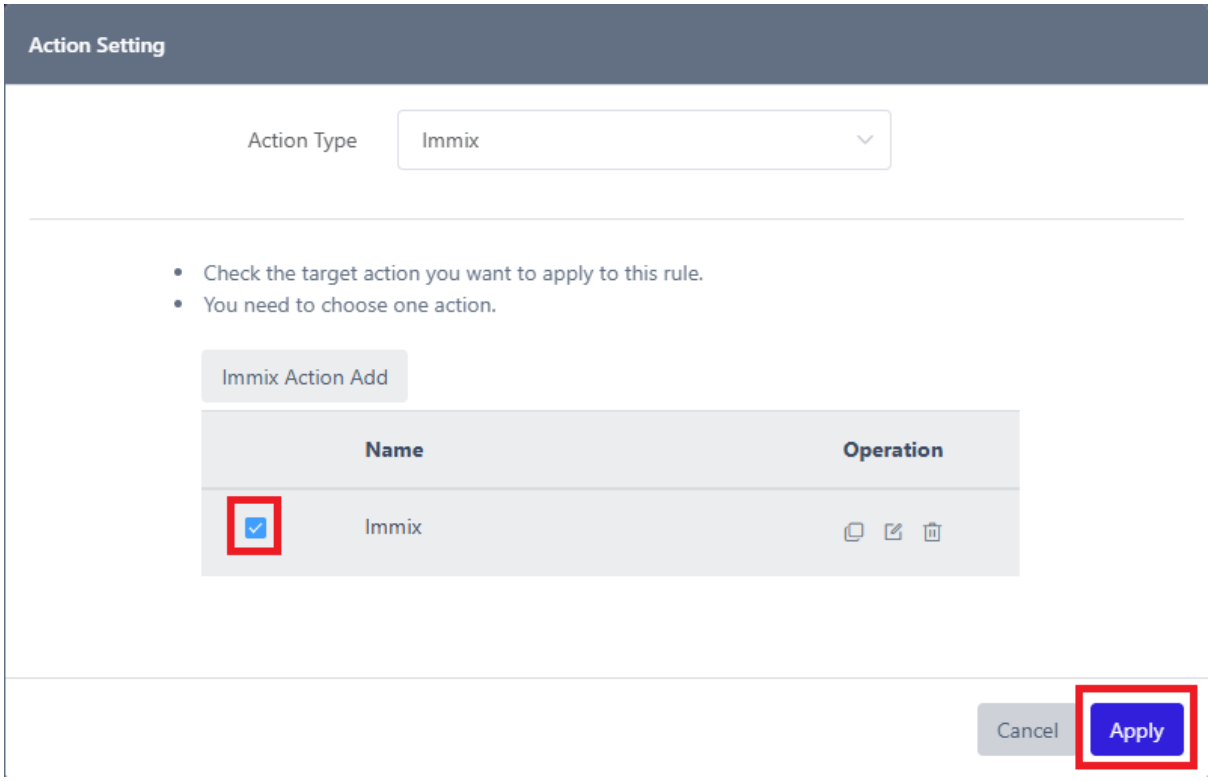
Once all settings are complete and the test is functioning correctly, click the “Apply” button.



Click the “OK” button.



Click the checkbox and then click “Apply.”

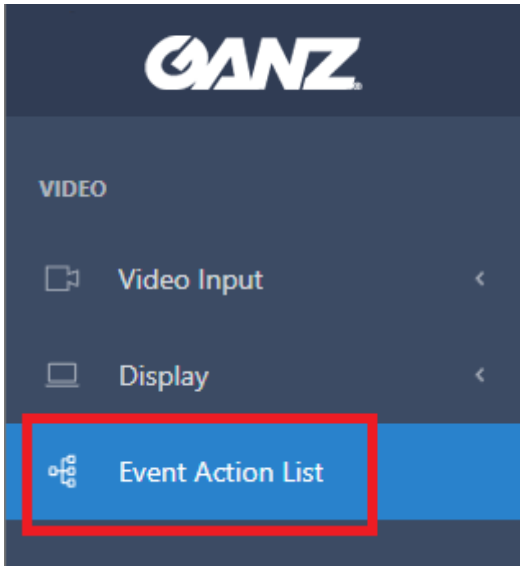


3. Demo

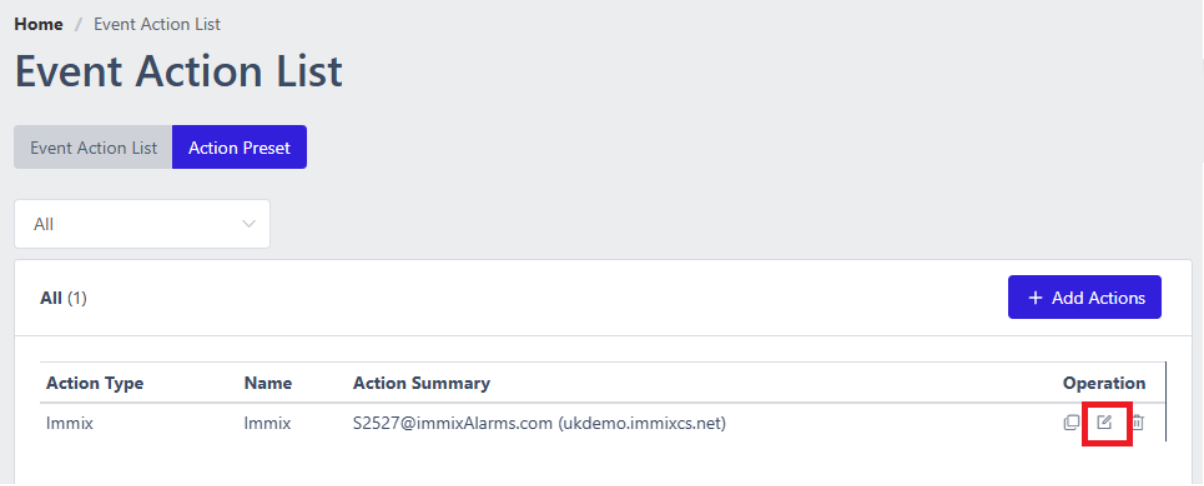
Now, you can check if the Event/Action is properly mapped.

3.1 Test using the AIBOX

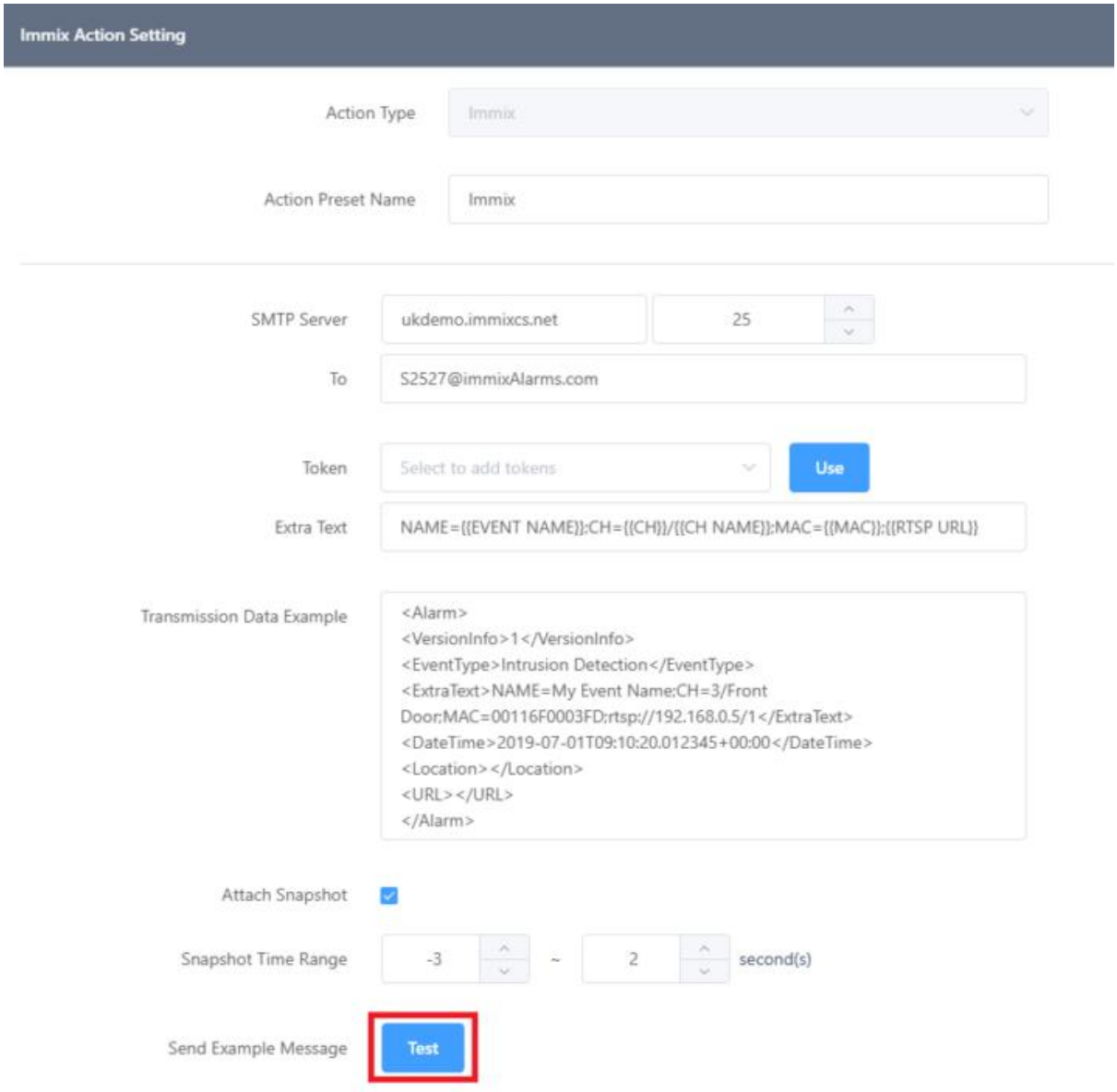
Access the AIBOX and click on “VIDEO” > “Event Action List” menu on the left sidebar.



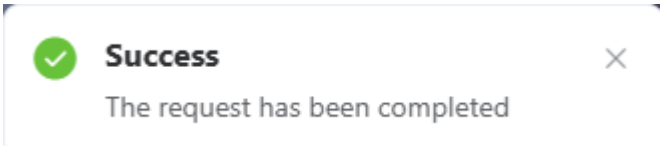
Click the “Edit” button in the previously created Immix action.



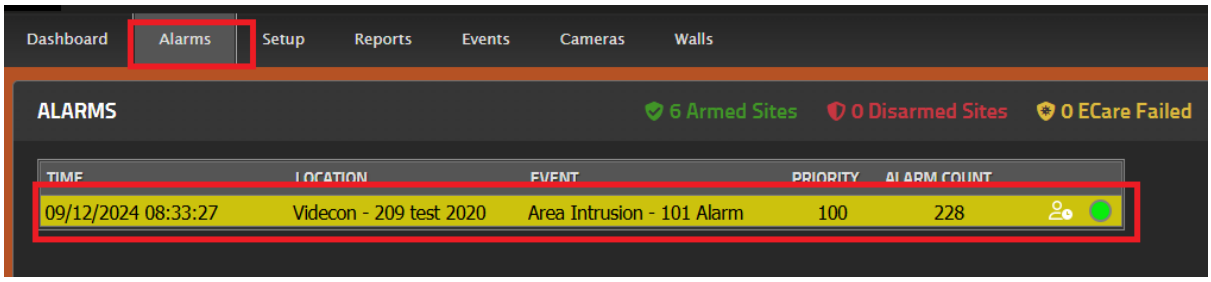
You can click the “Test” button to perform a test.



If the test is successful, a pop-up like the one below will appear.

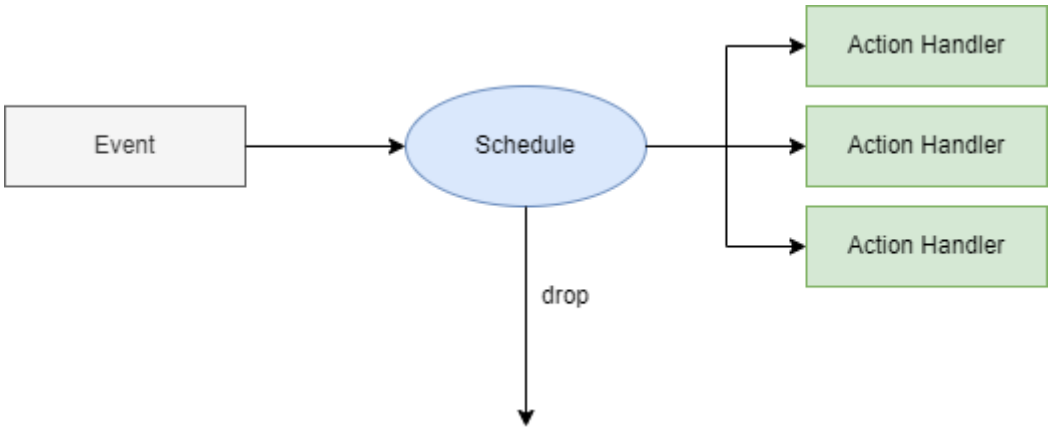


After logging into Immix, check the Alarm tab to confirm that the alarm has occurred. The test alarm will be triggered as Area Intrusion.



V. Schedule Setting Guide

A schedule can be set in all event action settings to trigger actions when events occur.



1. Schedule Overview

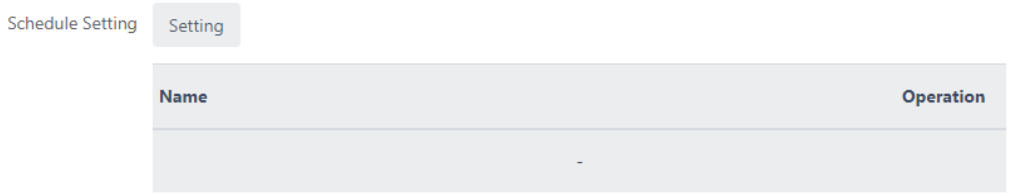
The schedule operates over a period of time to set the time for sending the notification whenever an event occurs. Depending on **weekly, monthly,** and **yearly** schedules can be set.
Additionally, specific dates can be designated as **exclusion schedules**. Actions will not be triggered during the exclusion schedule. Exclusion schedules are prior to regular schedules. This means that the action will not be triggered if an event occurs during a period that is included in both the exclusion and the regular schedule.

The schedule for event action settings operates according to the following policy.

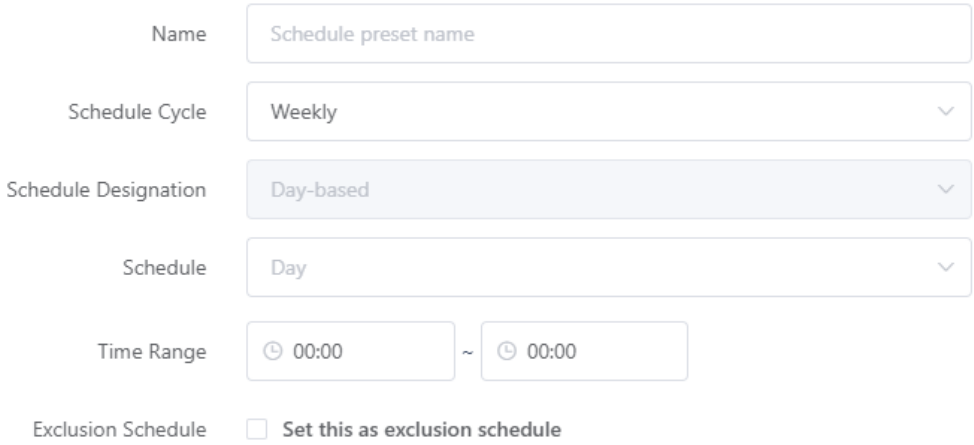
※ Schedule Application Policy
1. If no schedule is set in event actions, all events will always trigger the set action.
2. If multiple schedules are registered in event actions, the action will be triggered if one of them is true at least.
3. If an exclusion schedule is included, the action will not be triggered even if another schedule is true.
4. Schedules are set for each event action, but once created, they can be added in all event actions.

2. Create a New Schedule

1. Click the Setting button to add a schedule.



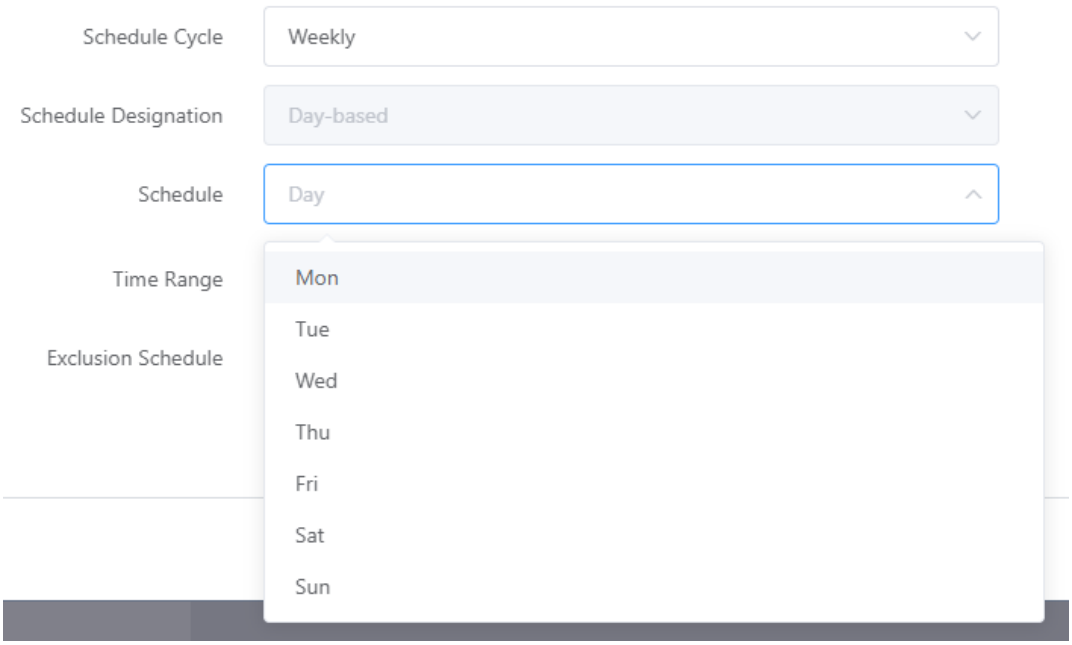
2. Click the Add New button to create a new schedule at the bottom.



Name : Enter a schedule name on “Name”(e.g. working hours, holidays).
Schedule Cycle : Set the “schedule cycle” for how often the schedule should repeat as weekly, monthly, or yearly.
Schedule Designation : Select whether the schedule is based on days of the week or specific dates.
Schedule & Time range : Set the days/dates/Time.
Exclusion Schedule : Check the box to set the schedule as an exclusion schedule.

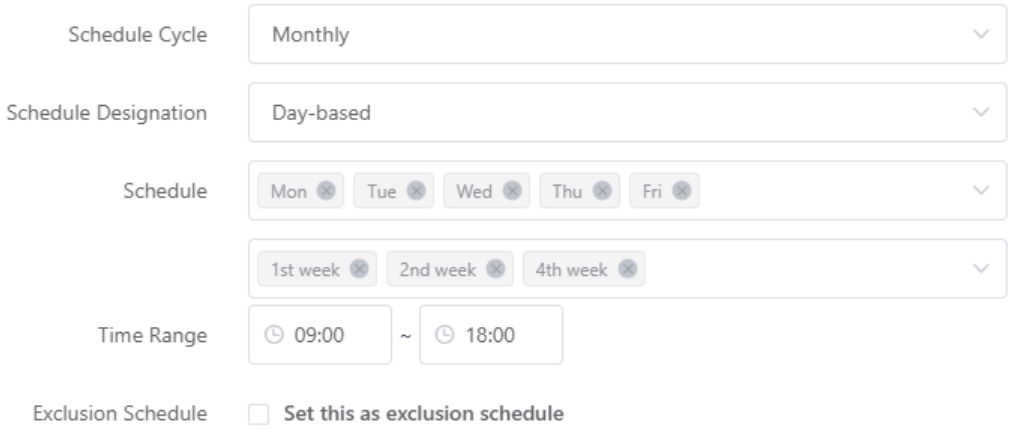
3. Weekly Schedule

1. Since weekly schedules cannot specify dates, the schedule Designation is fixed to Day-based of the week. You can set the target days and specify the time range to create a schedule. For example, you can set a schedule for **every Monday to Friday**.

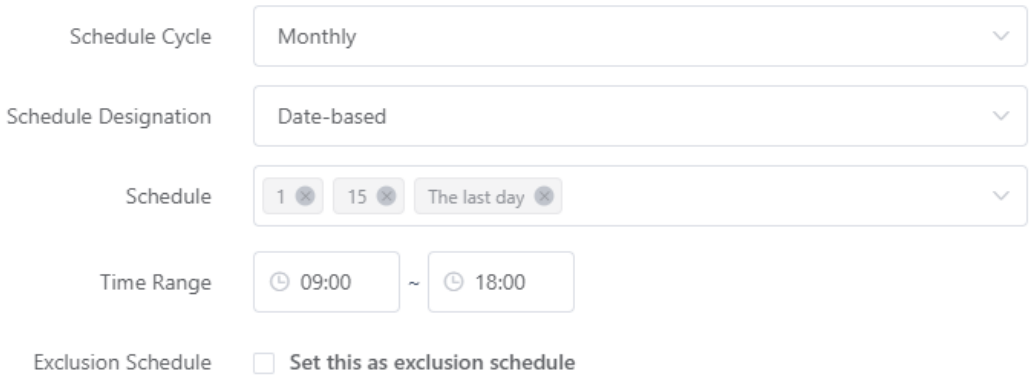


4. Monthly Schedule

1. For monthly schedules that use the Day-based option, you can specify by a week of the month. For example, you can set a schedule for **every second week of the month, Monday to Friday**.

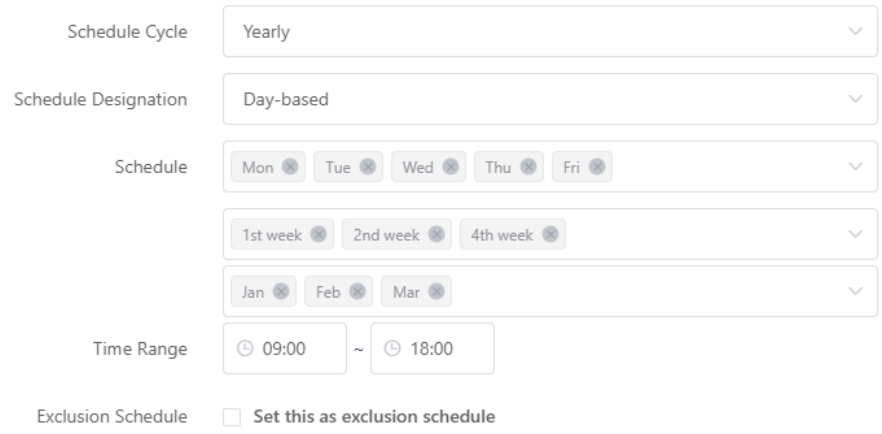


2. For monthly schedules that use the Date-based option, you can specify the dates of the month for the schedule. For example, you can set a schedule for the **1st, 15th, and the last day of the month.**

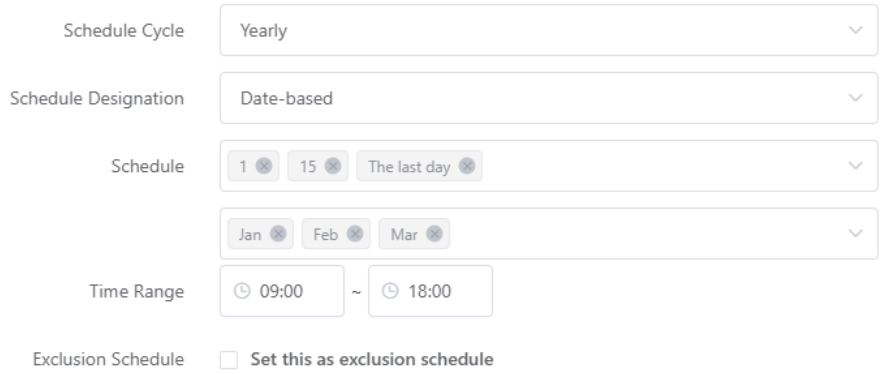


5. Yearly Schedule

1. For yearly schedules that use the Day-based option, you can specify the target month, week, and day. For example, you can set a schedule for **the second Monday to Friday of January to March every year.**



2. For yearly schedules that use the Date-based option, you can specify the dates for each target month. For example, you can set up a schedule on **the 1st, 15th, and the last day of January to March.**



6. Time Schedule Setting

The time schedule sets to run on the specified date. The time schedule follows the policy below.

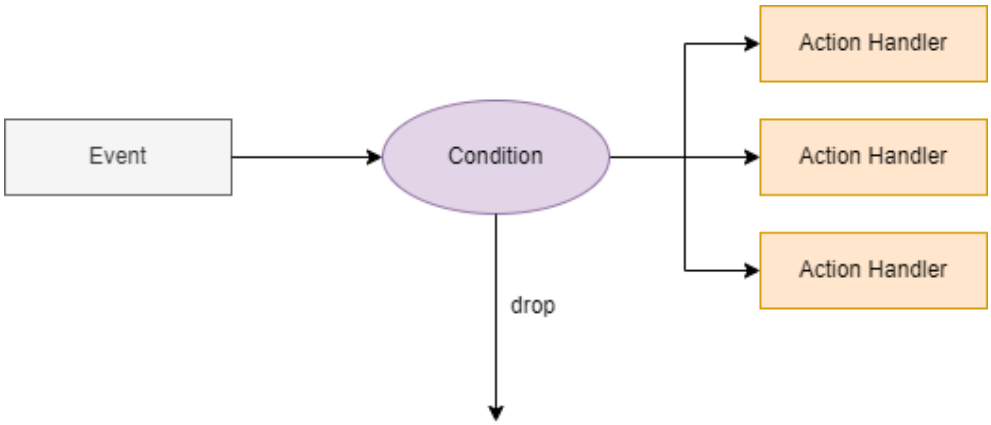
1. If the start time is faster then the end time, the schedule will be applied according to the specified time in the day. (e.g. 09:00~18:00)
2. If the start and end time are the same, the schedule will be applied for the entire 24 hours of that day. (e.g. 00:00~00:00)
3. If the start time is later than the end time, the schedule will be applied from the start time of that day until the end time of the next day. (e.g. 21:00~09:00)

7. Exclusion Schedule

You can set a schedule as an exclusion schedule, which takes priority over the regular schedule. If any of the exclusion schedules are active during the scheduled time of an event action, the action will not be triggered.

VI. Combined Rule Setting Guide

You can set compound rule conditions to trigger actions when events occur in event action settings.



1. Overview of Compound Rule Conditions

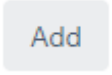
When setting up event action rules for each application, you can set conditions for triggering actions. In addition to setting scheduling conditions, you can also set conditions based on various system conditions to determine whether event actions should be triggered.
By utilizing the state of basic system resources such as alarm inputs or virtual alarm inputs, you can automatically control rules. If there are other event action settings that have been previously set up, you can also set conditions based on whether or not the event has occurred.
For example, if you want to turn on a warning light and broadcast a warning message to the camera through an alarm output for a residential intrusion event, you can reduce false alarms by setting the following conditions.

- Schedule (20:00~07:00)
- If even one person is detected outside the perimeter of the residential area within the last 10 seconds before the residential intrusion event occurs
- If alarm input signal 1 is being triggered

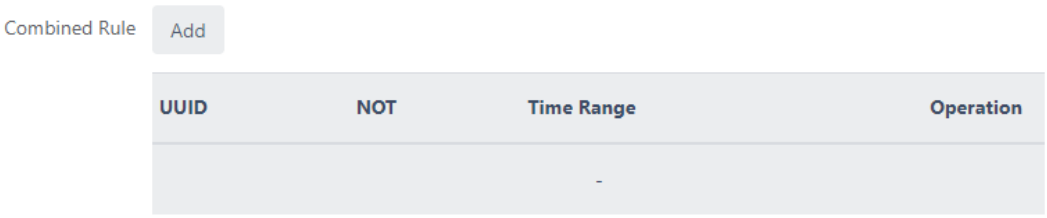
2. Combined Rule Conditions Setting

The following are the items that can be set as compound rule conditions

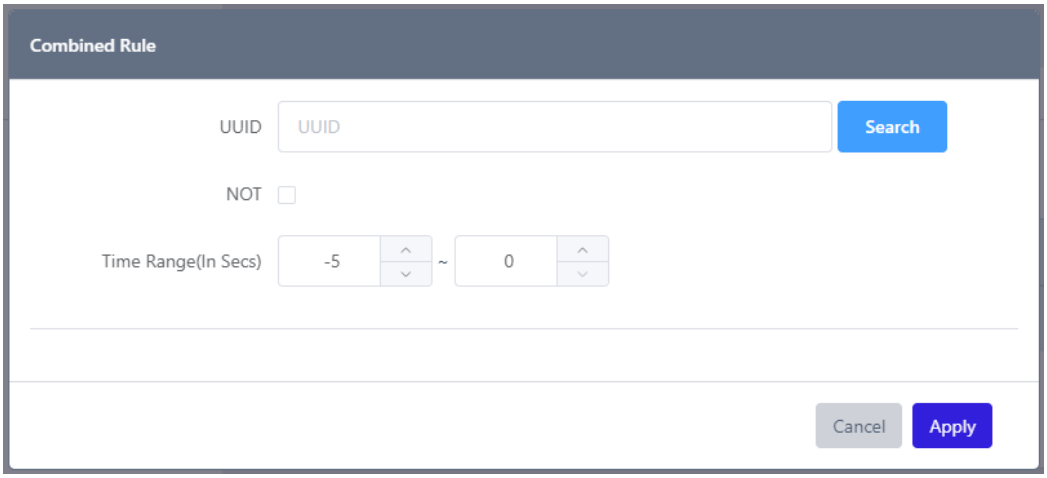
- Rules set up in the application
- Events specified by the application's rules.
- System I/O devices such as alarm inputs or virtual alarm inputs

1. Click the 

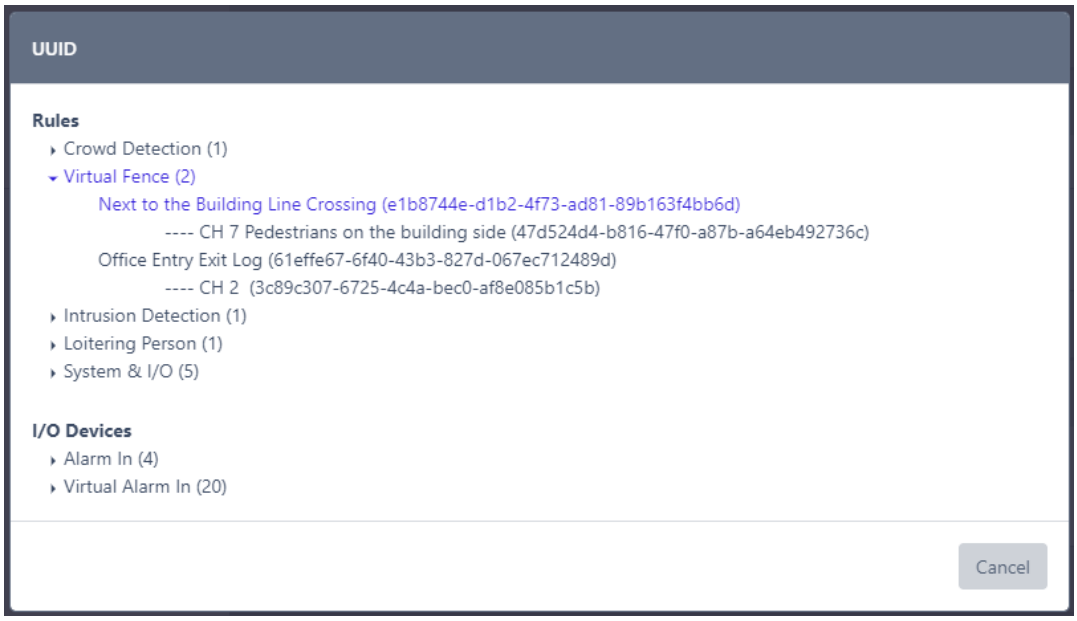
button to add a new condition on the event action setup screen.



2. Clik the Apply button to save after set the each options.



UUID : Ender the UUID value assigned to a target event, rule, or system device. When setting up an event action in the application, both the event and rule receive a unique UUID. You can input the UUID of the event or rule that you want to set up as a condition. Alternatively, Click Search button next to the UUID field allows you to search for and input a previously set-up item.



NOT : If NOT is checked, the condition will be true if the UUID event or rule is false. For example, if you specify the UUID of “Event A” and check the NOT checkbox, the condition will be true if “Event A” did not occur.

Time Range(In Secs) : Time Range field is used to set the valid time range for UUID events or rules. When an event for the rule occurs, if a UUID condition event occurs within the Time Range set based on the event occurrence time, the condition is considered true.

3. System I/O Combined Condition Settings

All rules and their events in currently used applications can be set as compound rule conditions.
Additionally, **alarm** and **virtual alarm inputs** can always be set as conditions for composite rules, even without setting up a separate event action rule.
These inputs have a unique resource UUID assigned to them in their initial state, and can be selected as a separate item in the UUID search UI.